Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme

Von der
Fakultät Architektur, Bauingenieurwesen und Umweltwissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig

zur Erlangung des Grades eines
Doktoringenieurs (Dr.-Ing.)
genehmigte

Dissertation

von
Gunnar Bosse
geboren am 8. April 1964
aus Wolfsburg

Eingereicht am 19. Mai 2010
Disputation am 23. November 2010

Berichterstatter Prof. Dr.-Ing. Jörn Pachl (TU Braunschweig)
Prof. Dr. sc. techn. Ulrich Weidmann (ETH Zürich)

2011

Inhaltsverzeichnis

Abstract ..... **v**

1 Motivation **1**

2 Ausgangssituation und Problemstellung **5**

2.1 Grundkomponenten der Eisenbahnen 5

2.2 Betriebsverfahren 7

2.2.1 Bedeutung für spurgeführte Verkehrssysteme 9

2.2.2 Einfluss auf die Sicherheit 12

2.3 Dokumentation des betrieblichen Systemwissens 14

2.4 Generisches Referenzsystem 15

3 Analyse betriebsverfahrensaffiner Funktions- und Gefährdungslisten **17**

3.1 Bilden einer einheitlichen Analysebasis 17

3.1.1 Wirkungskette 17

3.1.2 Wirkungskettenorientierte Darstellung der Risikodefinition 20

3.1.3 „Sanduhr“ 22

3.1.4 Vergleichende Gegenüberstellung 23

3.1.5 Modifizierte Sanduhr 24

3.2 Analyse generischer Listen 28

3.2.1 Generic Hazard List Methodology for Railway Signalling 28

3.2.2 ROSA – Rail Optimisation Safety Analysis 30

3.2.3 Fahrzeugfunktionen gemäß prEN 15380-4 35

3.2.4 EU-Interoperabilitätsrichtlinien und technische Spezifikationen (TSI) 44

3.3 Analyse spezifischer Projektlisten 47

3.3.1 Risikoanalyse FunkFahrBetrieb 47

3.3.2 Risikoanalyse Elektronisches Stellwerk 50

3.3.3 Risikoanalyse ETCS (Pilotanwendung) 53

3.4 Zusammenfassung der Analyseergebnisse 54

4 Vorgehen zum Definieren generischer Funktionen und Gefährdungen **57**

4.1 Architekturunabhängige generische Systemdefinition 57

4.1.1 Normative Vorgaben ... 58
4.1.2 Anforderungen für eine architekturunabhängige generische Systemdefinition ... 61
4.1.3 Beiträge zum Sicherheitsanalyseprozess gemäß EN 50129 ... 65
4.1.4 Bezug zu Einzelfallbetrachtungen ... 67
4.2 Formulierung generischer Funktionsdefinitionen ... 67
4.2.1 Anforderungen einschlägiger Normen ... 68
4.2.2 Anforderungen an das Definieren generischer Funktionen ... 69
4.2.3 Verwendung von Satzgliedern ... 72
4.2.4 Inhalt einer Funktionsdefinition ... 76
4.3 Identifizierung generischer Gefährdungen ... 78
4.3.1 Failure Mode and Effects Analysis ... 78
4.3.2 Anwendung der FMEA auf generisch definierte Funktionen ... 79
4.3.3 Modifizierte Gefährdungsidentifikation ... 82
4.3.4 Konzept für eine Ergebnis-FMEA ... 84
4.4 Funktionsgrundtypen ... 92
4.4.1 Erfüllung der Verkehrsaufgabe ... 93
4.4.2 Verbesserung der Sicherheit ... 93
4.4.3 Einfluss auf das Risiko ... 95
4.4.4 Tabellarische Übersicht ... 96
4.4.5 Umgang mit den Begriffen „Sicherheitsfunktion“ und „Schutzfunktion“ ... 97
4.5 Formular für das Definieren generischer Funktionen und Gefährdungen ... 99
4.5.1 Zweck ... 99
4.5.2 Zu erfassende Inhalte ... 99
4.5.3 Umsetzung ... 102
5 Anwendung ... 103
5.1 Definitionsbeispiele ... 103
5.1.1 Funktionales System ... 104
5.1.2 Betriebliche Funktionsgruppen ... 112
5.1.3 Betriebliche Grund- und Teilfunktionen ... 115
5.2 Beispiele für die Analyse definierter Funktionen ... 124

5.3 Erkenntnisse 126

6 Zusammenfassung 131

Literaturverzeichnis 135

Anhang 1: Analyse der „Starting Point Hazards“ (ROSA) 139

Anhang 2: Analyse der prEN 15380-4 (Code „G“) 141

Anhang 3: Analyse der prEN 15380-4 (Code „K“) 143

Anhang 4: Analyse der die prEN 150380-4 ergänzenden Funktionen (Code „L“) 146

Anhang 5: Liste generischer Betriebsverfahrensfunktionen (Auszug FWS) 149

Anhang 6: Hinweise zur Funktionsgruppe FWS 156

Anhang 7: Beispiele für die Analyse definierter Funktionen 157

Anhang 8: Funktionssteckbrief (Beispiel) 159

Anhang 9: Eingabemasken 160

Abkürzungsverzeichnis 162

Abstract

Track guided traffic systems consist somewhat simplified of infrastructure elements, rolling stock and operating procedures. Operating procedures are composed of operating rules and technical equipment to operate the rolling stock on the infrastructure. They are of particular importance both for operation and safety of track guided traffic systems. The operational safety depends on the safe functioning of the technical components as well as the safe acting of the staff.

Nevertheless, there exists up to now no catalogue which defines operating procedures comprehensively by generic functions and hazards. An important reason for this is the variety of different operating procedures in the railway domain. The differences are related not only to different operating philosophies but also to the various ways to achieve the operating procedures. Therefore, it is difficult to define the functions of operating procedures in a generic way. A conceivable way to solve this problem may be to define the operating procedures strong functionally without any relations to possible implementations. But for this, a high level of abstraction is needed.

In this thesis fundamentals are developed to ensure the needed level of abstraction. The elaborated procedural approach follows the IEC standard 61226 where “function” is defined as *„a specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it”.* Thus, the definition of generic functions requires a consideration of the motives to accomplish functions in railway systems.

Concerning the motives to accomplish functions in railway systems, the operational functions may be classified in elementary functional groups. According to the purpose of all traffic systems, at first there is a group of essential functions to accomplish the transport of persons and goods. Therefore they are called “basic functions” in this paper. The aim of the second functional group is the improvement of the system safety, called “functions to enhance safety” and is dependent on the technical solution. And third, there is a group of functions which serves a more efficient railway operation. Contrary to the first group, both the second and the third group are not needed in all cases.

The procedural approach elaborated in this thesis is based on the following aspects:

- Definition and differentiation of the functional groups “basic functions” and “functions to enhance safety” considering the European standards EN 50126 and EN 50129 as well as the “Recommendation on the 1st set of Common Safety Methods” issued by the European Railway Agency.
- Provide grammar-based means to ensure both purpose-oriented and implementation-independent definitions.

The applicability of the procedural approach is shown by defining interlocking functions and subfunctions (´interlocking´ is used in the sense of principles to achieve safe routes).

1 Motivation

Ein Betriebsverfahren ist ein „System betrieblicher Regeln und technischer Mittel zur Durchführung von Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur“ [PAC08-2]. Diese Definition umfasst die drei wesentlichen Elemente von Eisenbahnsystemen[1], mit denen jeweils spezifische Aufgabenstellungen realisiert werden: Die Fahrzeuge dienen der Aufnahme von Personen und Gütern und stellen die für die Ortsveränderung erforderlichen Antriebs- und Bremskräfte bereit; die Fahrweginfrastruktur wiederum trägt und führt die Fahrzeuge; mit Hilfe der Betriebsverfahren werden die Fahrten schließlich so koordiniert und gesteuert, dass für jede zugelassene Fahrt zwischen ihrem Start- und ihrem Zielort ein geeigneter Fahrweg, i.d.R. abschnittsweise, zur Verfügung steht und die Fahrzeuge nicht miteinander kollidieren. Die Betriebsverfahren sind sowohl aus operativen als auch die Sicherheit betreffenden Gründen von besonderer Bedeutung für die Eisenbahnsysteme. Der operativen Sichtweise folgend sind die Betriebsverfahren nicht allein auf das Bereitstellen zwingend erforderlicher operativer und sichernder Funktionen beschränkt, sondern können weitere Funktionen, wie z.B. zur Disposition umfassen. Dabei können, wie die Beispiele des Zugleiters im deutschen Zugleitverfahren und des Dispatchers nordamerikanischer Eisenbahnen zeigen, sicherheitsrelevante als auch disponierende Funktionen in einem Funktionsträger verschmelzen.

Obwohl die Betriebsverfahren von zentraler Bedeutung für den Betrieb von Eisenbahnsystemen und seine sichere Durchführung sind, ist festzustellen, dass es bislang keine umfassende und zusammenhängende generische Definition, Auflistung und Beschreibung der mittels Betriebsverfahren bereitzustellenden betrieblichen Funktionen gibt. Die besondere Schwierigkeit einer solchen Aufgabe scheint bei Betriebsverfahren darin begründet zu sein, dass die Betriebsverfahren im Gegensatz zu Fahrzeugen und Fahrweginfrastrukturen nicht ausschließlich aus technischen Funktionsträgern bestehen, sondern i.d.R. durch die Verknüpfung mit menschlichen Funktionsträgern realisiert werden. Die damit verbundene Möglichkeit, technische und menschliche Funktionsträger in mehr oder weniger beliebiger Weise miteinander kombinieren zu können, hat, *„obwohl die technischen Grundzüge des Funktionierens einer Eisenbahn überall gleich sind“* [PAC08-3], dazu geführt, dass sich die Architekturen von Betriebsverfahren wesentlich heterogener darstellen als jene von Fahrzeugen und Fahrweginfrastrukturen.

[1] Die in dieser Arbeit gemachten Ausführungen gelten nicht nur für das System Eisenbahn, sondern lassen sich, wie mit dem Titel der Arbeit unterstrichen wird, ihrem Grundsatz nach auch auf alle anderen spurgeführten Verkehrssysteme übertragen. Der sprachlichen Einfachheit halber und dem fachlichen Umfeld der Entstehung dieser Arbeit Rechnung tragend werden nur der Begriff „Eisenbahn“ und daraus abgeleitete Begriffe verwendet.

Im Rahmen der zunehmenden Internationalisierung des Eisenbahnwesens nimmt der Bedarf nach einer generischen Beschreibung betrieblicher Funktionen und Gefährdungen aus mehreren Gründen zu. Wichtige Gründe sind u.a.:

- Die Internationalisierung der Eisenbahnlehre benötigt von den nationalen Sichtweisen abstrahierende Beschreibungen, die sowohl das Funktionieren als auch das Verhalten der Eisenbahnsysteme beim Versagen der Funktionen auf einem allgemeingültigen Gerüst aufbauend zeigen und von einem solchen Verständnis heraus einen vergleichenden Blick auf die jeweiligen nationalen Lösungen und Unterschiede erlauben.
- Für den zwar langfristigen, aber notwendigen Prozess einer europaweiten Angleichung von Betriebsverfahren wird als Referenz eine Art Musterbetriebsverfahren benötigt, dem die bislang heterogen gestalteten Betriebsverfahren nach und nach angeglichen werden könnten.
- Für die Standardisierung von Regelwerksstrukturen werden technikneutral beschriebene Verfahrensregeln benötigt; vgl. a. [BRA10]. Sie können z.B. im sprachgrenzüberschreitenden Verkehr das Sprachverständnis von nichtmuttersprachlichem Betriebspersonal erleichtern.
- Auch die Vorgabe einheitlicher Sicherheitsziele in Europa bedarf einer einheitlichen Definitions- und Bezugsbasis, die sich auf den Grundzügen des Funktionierens der Eisenbahn als kleinsten gemeinsamen Nenner abstützt. Ziel muss es sein, diese Basis, soweit generisch vertretbar, möglichst detailliert zu definieren, dabei aber Realisierungsbezüge zu vermeiden.

Die Definition einer funktionalen Referenz oder umfassender eines Referenzsystems, die oder das trotz der bestehenden Heterogenität generische Funktionen und Gefährdungen enthält, bedarf eines sehr hohen Abstraktionsniveaus, das von den beteiligten Fachleuten ein gedankliches Loslösen von den eigenen, i.d.R. national, unternehmerisch und technischen Einrichtungen geprägten Denkweisen und Betriebsverfahren erfordert. Dies ist vor dem Hintergrund einer bislang vergleichbar heterogen Ausbildung im Eisenbahnwesen als eine nicht zu unterschätzende Hürde beim Erstellen einer funktionalen Referenz anzusehen.

Einen bereits vergleichsweise ausgeprägten länderübergreifenden Ansatz beinhalten z.B. die dem Führen von Sicherheitsnachweisen dienenden Normen EN 50126 und EN 50129. Die im Abschnitt 3 dieser Arbeit durchgeführte Analyse von Risikoanalysen und generischen Gefährdungslisten zeigt jedoch, dass es sich bei diesen Listen im Wesentlichen um durch die jeweiligen Systemdefinitionen vorgeprägte Unikate handelt und der generische Anspruch sich weitgehend nur auf die Realisierung der zu entwickelnden Funktionsträger bezieht. Zudem scheint der Ansatz der Normen, die Identifikation der vom zu entwickelnden System mit ausreichender Sicherheit zu beherrschenden Gefährdungen in den Vordergrund zu stellen, zu einer verhältnismäßig starken Fokussierung auf den Aspekt „Sicherheit“ zu führen, hinter dem die operativen Aspekte des Eisenbahnbetriebs in den Hintergrund zu treten scheinen.

Die überall gleichen technischen Grundzüge des Funktionierens der Eisenbahn drücken sich jedoch, so die vom Autor dieser Arbeit vertretene These, dem Zweck eines Verkehrssystems entsprechend und naturgesetzlichen Grundlagen Rechnung tragend zunächst einmal in Funktionen aus, die operativer Natur sind. Die für die Ortsveränderung erforderlichen Funktionen scheinen deshalb in einem besonderen Maße geeignet zu sein, die Ausgangsbasis für die Definition einer generischen Referenz zu bilden. Die Nutzer der Verkehrssysteme erwarten natürlich, dass diese operativ geprägten Funktionen ihrem Sicherheitsempfinden entsprechend sicher ausgeführt werden. Gegebenenfalls müssen sie zum Erreichen der erwarteten Sicherheitsziele durch ergänzende Funktionen flankiert werden. Diese ergänzenden Funktionen greifen in die die Sicherheit beeinflussenden Wirkungszusammenhänge ein, die beim gefährlichen Versagen der operativ geprägten Funktionen, ausgehend von den verursachenden Fehlern und Ausfällen bis hin zu den möglichen Unfällen und ihren Schadensausmaßen, ablaufen. Somit lässt sich das sichere Erbringen von Verkehrsleistungen in einem Verkehrssystem als eine Verflechtung operativer Prozesse mit sicherheitsrelevanten Wirkungszusammenhängen auffassen und die Sammlung generischer Funktionen um entsprechende sicherheitsfördernde Funktionen erweitern.

In dieser Arbeit werden Grundlagen zur generischen Identifikation und Beschreibung der in spurgeführten Verkehrssystemen durch Betriebsverfahren realisierten Funktionen entwickelt, die auf einer durch operative Zwecke geprägten Systembetrachtung aufbauen und die die sicherheitsrelevanten Wirkungszusammenhänge einbeziehen, die auch der den Normen EN 50126 und EN 50129 ensprechenden „Sanduhr“ zugrunde liegen.

Im Kapitel 2 dieser Arbeit wird unter Einbeziehung eines entwicklungsgeschichtlichen Rückblicks zunächst die Bedeutung der Betriebsverfahren erläutert und darauf aufbauend die Problem- und die Aufgabenstellung hergeleitet. Zur Beschreibung der Ausgangsituation werden im Kapitel 3 betriebsverfahrensaffinine Funktions- und Gefährdungslisten analysiert. Im Kapitel 4 werden Grundlagen geschaffen, die dem Definieren einer generischen Referenz dienen sollen. Ihre prinzipielle Anwendbarkeit wird im Kapitel 5 anhand eines praxisnah mit Experten durchgeführten Beispiels demonstriert. Die Ergebnisse und die im Laufe dieser Arbeit gewonnenen Erkenntnisse werden im Kapitel 6 zusammengefasst, eine Einordnung der Arbeit vorgenommen und ein Ausblick gegeben.

2 Ausgangssituation und Problemstellung

2.1 Grundkomponenten der Eisenbahnen

Das Institut für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig erläutert seit mehreren Jahren auf einer insbesondere an Studierende jüngerer Semester gerichteten Internetseite den Aufbau des Systems Eisenbahn, um daran eine Einordnung seines Lehrangebots vorzunehmen [IfEV01]. Der Systemaufbau wird mit Hilfe einer einfachen, vom Verfasser dieser Arbeit entworfenen, grafischen Darstellung in Dreiecksform symbolisiert. Im Mittelpunkt des aus vier gleichseitigen Dreiecken bestehenden Dreiecks befindet sich der Begriff „Eisenbahnbetrieb“, der von den drei auch für fachliche Laien augenfälligen Eisenbahnkomponenten „Fahrzeuge“, „Bauliche Infrastruktur“ sowie „Leit- und Sicherungstechnik“ umgeben wird (Bild 1).

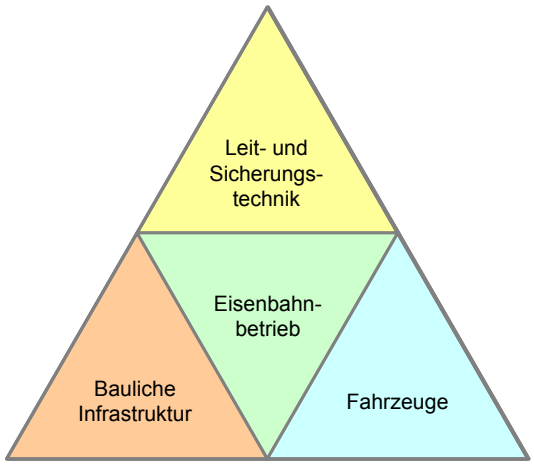


Bild 1: Einfache Darstellung des Systems Eisenbahn

Das mittlere Dreieck symbolisiert das Zusammenwirken von Fahrzeugen, baulicher Infrastruktur[2] und Leit- und Sicherungstechnik, durch das der Betrieb von Eisenbahn realisiert wird. Da weder die Fahrzeuge noch die Fahrweginfrastruktur noch die Leit- und Sicherungs-

[2] Die bauliche Infrastruktur umfasst alle baulich-konstruktiven Elemente, die von Fahrzeugen im weitesten Sinne „befahren“ werden (z.B. Fahrbahn einschließlich umgebenden Lichtraum, Brücken und Tunnel), der Versorgung der Fahrzeuge mit Antriebsenergie (z.B. Fahrleitungsanlagen) und der Aufnahme und Abgabe von Transportgütern und Personen dienen (Ladeeinrichtungen, Bahnsteiganlage, Gebäude). Konstruktive Elemente und Anlagen, deren Funktionen der Leit- und Sicherungstechnik zuzurechnen sind (z.B. Signalanlagen, Stellwerke), werden nicht der baulichen Infrastruktur zugeschlagen. Diese Aufteilung der Teilsysteme steht bis auf die Zuordnung der Versorgung mit Antriebsenergie zur Infrastruktur in Übereinstimmung mit der europäischen Richtlinie über die Interoperabilität des konventionellen transeuropäischen Eisenbahnsystems. Dort wird „Energie“ als ein eigenes Teilsystem definiert [2008/57/EG, Anhang II].

technik für sich allein wirken und den Betrieb des Systems Eisenbahn bestimmen können, liegt es auf der Hand, dass dieses Zusammenwirken in geeigneter Weise geregelt werden muss. Wesentliche Elemente des mittleren Dreiecks „Eisenbahnbetrieb“ sind folglich betriebliche Regeln, mit denen der Verkehr von Fahrzeugen auf der Fahrweginfrastruktur „organisiert“, d.h. geleitet und gesichert wird. Die Dreiecke können somit in leicht veränderter Interpretation der Darstellung auch als die vier grundlegenden Komponenten des Systems Eisenbahn aufgefasst werden.

Die Aufgaben der Fahrzeuge und der baulichen Infrastruktur sind elementar. Sie sind für das System unverzichtbar. Dies gilt auch für die betrieblichen Regeln, deren Anwendung und Einhaltung für einen ordnungsgemäß geleiteten und gesicherten Betrieb notwendig ist. Die Leit- und Sicherungstechnik ist, zumindest theoretisch, verzichtbar. So ist ein primitives Eisenbahnsystem vorstellbar, das allein aus Fahrzeugen, baulicher Infrastruktur und betrieblichen Regeln, deren Anwendung und Einhaltung allein durch den Menschen realisiert wird, besteht (Bild 2).

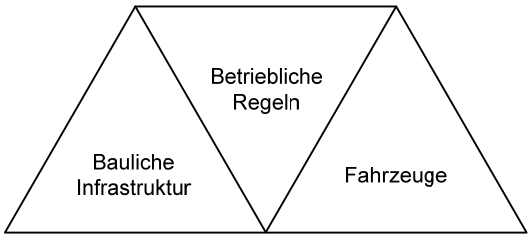


Bild 2: Elemente eines primitiven Eisenbahnsystems

Ohne den Ausführungen des Abschnittes 2.2 vorgreifen zu wollen, sei an dieser Stelle festgehalten, dass die Realisierung der betrieblichen Regeln allein durch den Menschen die aufgrund des Leistungspotenzials der Fahrzeuge und der baulichen Infrastruktur mögliche Leistungsfähigkeit sowie die Sicherheit des Systems Eisenbahn erheblich einschränken würde. Deshalb werden bei allen modernen Eisenbahnen technische Hilfsmittel genutzt, mit denen das Leiten und Sichern unterstützt bzw. durchgeführt wird. Die betrieblichen Regeln und die Leit- und Sicherungstechnik stehen folglich in einer engen Wechselwirkung zueinander. Betrachtet man verschiedene Realisierungen, wie z.B. den Zugleitbetrieb und die LZB-Führung, so fällt auf, dass es im Gegensatz zu den Fahrzeugen und zur baulichen Infrastruktur keine allgemeingültige Abgrenzung zwischen den beiden Dreiecken „Betriebliche Regeln“ und „Technische Hilfsmittel“ gibt. Ihr Miteinander ist in nahezu beliebiger Vielfalt kombinierbar und führt letztlich zu verschiedenen Lösungen. Im Bild 3 wird dies durch eine gestrichelte Linie und einen auf beide Dreiecke weisenden Pfeil symbolisiert. In Summe müssen jedoch beide Dreiecke alle zum Leiten und Sichern der jeweiligen Eisenbahn erforderlichen Funktionen enthalten. In dieselbe Richtung zielt MASCHEK und greift in [MAS09] ebenfalls das Sinnbild des Dreiecks auf. Er drückt den Sachverhalt dahingehend aus, dass *„Betrieb“* und *„LST“ „untrennbar miteinander verbunden“* seien.

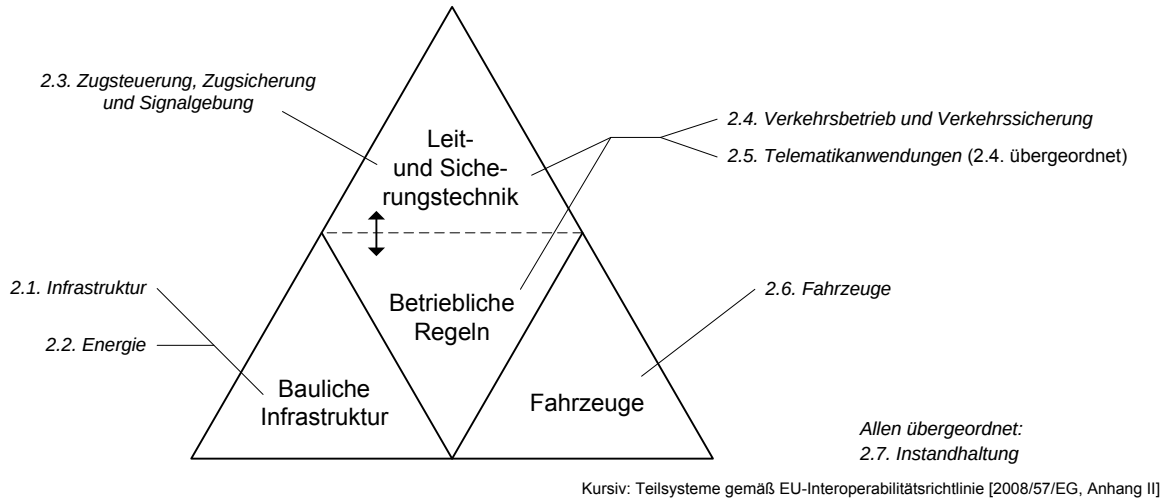


Bild 3: Grundelemente moderner Eisenbahnsysteme

Das zuvor erläuterte und im Bild 3 dargestellte Modell des Systems Eisenbahn liegt den weiteren Ausführungen dieser Arbeit als Gedankenbasis zugrunde. Die in der EU-Interoperabilitätsrichtlinie definierten Teilsysteme können dem Dreieck zugeordnet werden.

2.2 Betriebsverfahren

NAUMANN und PACHL definieren in [NP02, S. 33] den Begriff Betriebsverfahren als ein *„System betrieblicher Regeln und technischer Mittel zur Durchführung von Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur“*. MASCHEK verweist in einer neueren Veröffentlichung auf die im Rahmen der Risikoanalysen FFB und ETCS eingeführte *„Kategorie ‚LST und Betrieb'“*. Er stellt dazu jedoch fest, dass sich *„eine einheitliche Bezeichnung des beschriebenen Sektors bisher noch nicht herausgebildet“* habe [MAS09]. BRABAND wiederum nutzt im Zusammenhang mit der RA FFB den Begriff „Betriebsverfahren“ [BRA05, S. 82]. Der Autor der vorliegenden Arbeit wird den Begriff *„Betriebsverfahren*“ im von NAUMANN und PACHL definierten sowie im Bild 4 dargestellten Sinne nutzen und versteht den Begriff *„Betrieb“* als das Zusammenwirken aller vier Dreiecks-Komponenten.

Um die Bedeutung der Betriebsverfahren für das System Eisenbahn und ihre Natur zu unterstreichen, verwendet PACHL die Analogie zur Computertechnik [PAC05, S. 1], [PAC08-4, S. 32]. Hiernach umfasst die *„Hardware“* des Systems Eisenbahn i.d.R. netzartige Fahrweginfrastrukturen und die darauf verkehrenden Fahrzeuge. Um die Fahrten der Fahrzeuge auf der Fahrweginfrastruktur durchführen zu können, werden als *„Software“* Betriebsverfahren benötigt. Das Sinnbild von Hard- und Software ist gut mit der Dreieckdarstellung des Systems Eisenbahn in Übereinstimmung zu bringen (Bild 4).

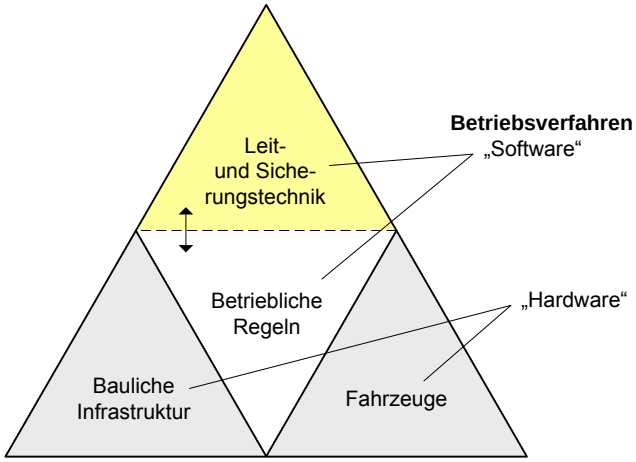


Bild 4: Betriebsverfahren als „Software“ des Systems Eisenbahn

Mit Hilfe der Betriebsverfahren werden betriebliche Funktionen realisiert, durch die u.a. zu gewährleisten ist, dass für die Fahrten zwischen den Start- und Zielpunkten geeignete Fahrwege zur Verfügung stehen und dass keine materiellen Konflikte zwischen den Fahrzeugen auftreten. Anderenfalls ist durch die Betriebsverfahren sicherzustellen, dass die Fahrten nicht stattfinden. Die ebenfalls für das Durchführen der Fahrten erforderlichen Funktionen zum Erzeugen der Antriebs- und Bremskräfte sowie die Trag- und Führungsfunktionen der Fahrweginfrastruktur werden nicht zu den Betriebsverfahren gezählt, sondern werden als elementare Funktionen der „Hardware“-Komponenten betrachtet. Die Betriebsverfahren decken die in der Interoperabilitätsrichtlinie der EU definierten Teilsysteme „Zugsteuerung, Zugsicherung und Signalgebung“ und „Verkehrsbetrieb und Verkehrssteuerung“ ab [2001/16/EG, Anhang II].

So wie es z.B. für die Aufgabe auf einem Computer einen Text zu schreiben, verschiedene Textverarbeitungsprogramme gibt, die auf derselben Computerhardware, d.h. unter Nutzung derselben Ein- und Ausgabemedien, Prozessoren usw. laufen, so fallen auch die Betriebsverfahren unterschiedlich aus. Die Möglichkeit der Zuscheidung von Funktionen an menschliche und technische Funktionsträger hat im Laufe der Entwicklung des Eisenbahnwesens aus technischen und betriebsphilosophischen, aber auch politischen und militärstrategischen Gründen weltweit zu einer Vielzahl von Betriebsverfahren geführt, die sich hinsichtlich der betrieblichen Regeln, der technischen Hilfsmittel und der Technisierungsgrade (Bild 5) unterscheiden; vgl. auch [PAC08-3].

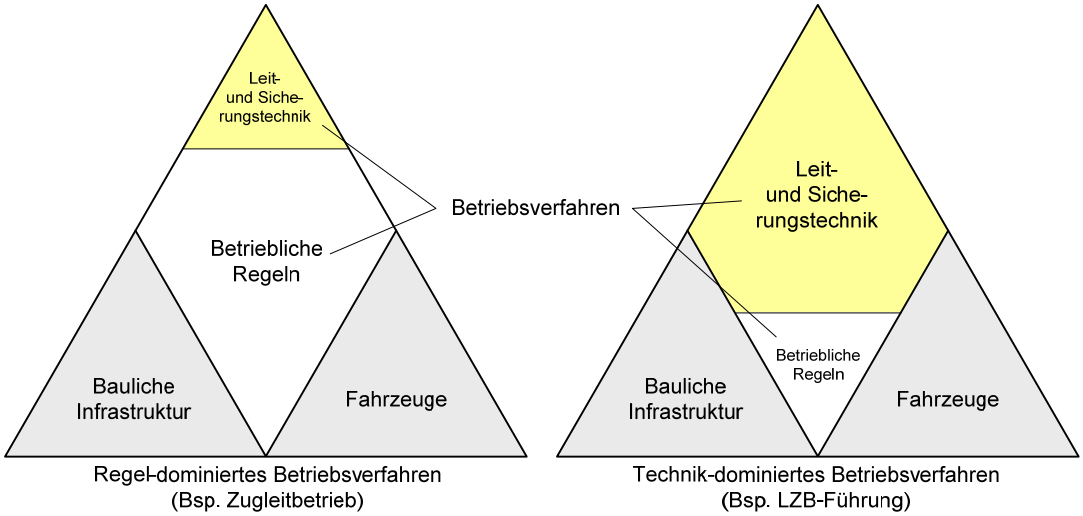


Bild 5: Betriebsverfahren mit unterschiedlichen Technisierungsgraden

2.2.1 Bedeutung für spurgeführte Verkehrssysteme

Die vorstehend beschriebene Computer-Analogie lässt sich prinzipiell auch auf alle anderen Landverkehrssysteme sowie auf die Schiff- und Luftfahrt anwenden. Allerdings besitzen die Betriebsverfahren für spurgeführte Verkehrssysteme systembedingt eine so große Bedeutung, dass man sie als ein wesentliches Charakteristikum spurgeführter Verkehrssysteme betrachten kann.

Der heutzutage z.T. vergleichsweise hohe Anteil sicherungstechnischer Hilfsmittel innerhalb der Betriebsverfahren darf nicht dazu führen, die Betriebsverfahren als sicherungstechnischen Selbstzweck der Eisenbahn aufzufassen und sie dem eigentlichen operativen Zweck des Transportssystems Eisenbahn, Ortsveränderungen von Personen und Gütern sicher zu erbringen, überzuordnen. Deshalb soll zunächst mit dem folgenden entwicklungsgeschichtlichen Rückblick der operative Charakter der Betriebsverfahren unterstrichen werden.

2.2.1.1 Entwicklungsgeschichtlicher Rückblick

Die Bedeutung von Verfahren zur Organisation des Fahrbetriebes wurde bereits in der Frühzeit des Eisenbahnwesens nach einer anfänglichen Experimentierphase erkannt. SCHIVELBUSCH gibt in [SCH02] einen interessanten Einblick in eine eisenbahngeschichtliche Entwicklungsphase, die man mit „Entdeckung der Betriebsverfahren“ charakterisieren könnte. Dieser Rückblick schärft durch die darin zitierten, mitunter bildhaft formulierten Quellen das Verständnis für die bis heute geltenden betrieblichen Charakteristika spurgeführter Verkehrssysteme. Im Folgenden werden die Ausführungen SCHIVELBUSCHs auf Betriebsverfahren bezogen zusammengefasst und der Bezug zum heutigen Stand der Technik, d.h. einer fahrwegseitigen Prägung der Betriebsverfahren, hergestellt.

Mit den in der industriellen Revolution im 19. Jahrhundert hervorgebrachten Technologien sind zunächst im „Hardware-Bereich“ der Eisenbahn die grundlegenden technologischen

Rahmenbedingungen geschaffen worden. Dazu gehören insbesondere die durch die Fahrzeuge und die Fahrweginfrastruktur geprägten Eigenschaften wie eine hohe Antriebsleistung, die Spurführung und die dadurch geschaffene Möglichkeit der Zugbildung. Mit diesen Eigenschaften revolutionierte die Eisenbahn den bis dahin mit Kutschen, Pferden und zu Fuß abgewickelten Landverkehr.

Die revolutionäre Veränderung des damaligen Verkehrsgeschehens betraf nicht nur die hervorgerufene Erhöhung der Transportleistungen, sondern sie veränderte auch seine bis dahin durch Liberalität geprägte Abwicklung. Denn sowohl in betrieblicher Hinsicht als auch im ökonomischen Denken entsprach der Landverkehr bis zum Erscheinen der Eisenbahnen weitgehend Individualverkehrssystemen heutiger Prägung: Die damaligen Verkehrsmittel waren auf ihren Fahrwegen frei beweglich, d.h. sie konnten einander an nahezu jeder beliebigen Stelle ausweichen. Auch wurden sie im freien Ermessen des jeweiligen Betreibers, Besitzers oder Fahrers eingesetzt und wirtschaftlich verantwortlich betrieben. An die Eigentümer der Fahrweginfrastruktur wurden gegebenenfalls Nutzungsgebühren gezahlt. Die Ausführungen zum damaligen Landverkehr gelten in den wesentlichen Zügen auch für den seinerzeit ebenfalls bedeutenden Verkehr auf Flüssen und Kanälen.

Maschinenartiger Verbund

Die Entwicklung der Eisenbahnen war, um das operative Ziel der Ortsveränderung von Personen und Gütern zu erreichen, zunächst durch die Entwicklung der technischen Komponenten wie Fahrzeuge und Fahrweg geprägt. Mit der Spurführung wurde jedoch ein für damalige Verhältnisse neuartiger, enger technischer Verbund zwischen Fahrzeug und Fahrweg geschaffen, den REULEAUX 1875 als einen Entwicklungsschritt bezeichnete, *„welcher Wagen und Weg zur Maschine vereinigte“*[3]. Dieser damals als maschinenartig empfundene Verbund schloss ein beliebiges Ausweichen einander entgegenkommender Fahrzeuge ebenso aus wie das freie Überholen eines langsameren Fahrzeugs.

Das mit der Eisenbahn geschaffene neue Verkehrssystem wies also gravierende Unterschiede auf, die mit den seinerzeitigen liberalen Vorstellungen und Betriebsweisen nicht im Einklang standen. Dies führte letztlich bereits in der ersten Hälfte des 19. Jahrhunderts zu bis dahin im Verkehrswesen unbekannten betrieblichen Organisationsformen.

Notwendigkeit einer einheitlichen Betriebsführung

Angesichts des neuartigen Verbunds von Fahrweg und Fahrzeug wurde schon relativ bald deutlich, dass sich das neue System auch in seiner Betriebsabwicklung grundlegend von den bisherigen Verkehrsmitteln unterscheiden müsse. Um den liberal geprägten Verkehrsvorstellungen nicht zuwider zu laufen, wurde für die Eisenbahnen u.a. vorgeschlagen, je Fahrtrichtung mehrere Gleise parallel zu verlegen. So hielt GRAY 1825 in der unmittelbaren

[3] Reuleaux, Franz: Theoretische Kinematik, Grundzüge einer Theorie des Maschinenwesens. Vieweg-Verlag, Braunschweig 1875, S. 231, zitiert in [SCH02, S. 23]

Umgebung von London *„womöglich sechs Schienenstränge“ für erforderlich, „um eine Eisenbahn für den allgemeinen Verkehr durchzusetzen“*[4].

Solche infrastrukturintensiven Projekte sind in damaliger Zeit allerdings nicht umgesetzt worden. Vielmehr erwuchs aus den negativen Erfahrungen mit liberal geprägten Betriebsweisen die von LARDNER 1851 rückblickend formulierte Erkenntnis, dass *„das neue Verkehrsmittel Eigenschaften besaß, die einen ungeregelten Fuhrbetrieb ausschlossen. Eine Eisenbahn, die wie eine große Maschine arbeitet, deren Teile miteinander aufs engste verbunden sind und deren Bewegungen ein bestimmtes Minimum von Einheitlichkeit verlangen, kann aus diesem Grunde nicht von einer Anzahl voneinander unabhängiger Agenten betrieben werden. Ein derartiges System würde sich sehr schnell selbst vernichten“*.[5] LARDNER kommt im selben Dokument zu folgendem Schluss:

„Der Betrieb der Eisenbahn erfordert eine einheitliche Leitung und aufeinander abgestimmte Bewegungen, und das ist nur zu erreichen durch eine Zusammenfassung des gesamten Fuhrbetriebes und der allgemeinen Verwaltung der Bahn.“

Mit dieser Formulierung wurde zum Ausdruck gebracht, dass das neue Verkehrssystem neben den Fahrzeugen und dem Fahrweg eine weitere Komponente besaß: Den Betrieb und seine Führung, die durch eine entsprechende Organisationsform zu gestalten sei. Mit Begriffen wie *„einheitliche Leitung“*, *„aufeinander abgestimmte Bewegungen* [A.d.V.: der Fahrzeuge]*“*, sowie *„Zusammenfassung des gesamten Fuhrbetriebes“* und *„allgemeine Verwaltung“* wird von ihm der Betrieb nicht als gegenständliches Element beschrieben, sondern es lässt sich eine „weiche“ Komponente, die Betriebsführung erkennen. Diese Sichtweise besteht in der heutigen Eisenbahnpraxis sowie in der Eisenbahnwissenschaft und –lehre unverändert fort. So versteht z.B. PACHL als Betriebsführung ein *„system of operating rules and procedures for a safe and efficient operation“* [PAC05, S. 1].

2.2.1.2 Charakterisierung aus heutiger Sicht

Die heutigen Bestrebungen z.B. in Europa, den Eisenbahnmarkt zu liberalisieren, indem vormals staatliche Eisenbahnen in privatwirtschaftlich getrennt organisierte Eisenbahninfrastruktur- (EIU) und Eisenbahnverkehrsunternehmen (EVU) überführt werden, scheinen den Forderungen LARDNERs nach einer einheitlichen Leitung auf den ersten Blick entgegenzustehen. Dieser Eindruck mag seine Ursache darin haben, dass heutzutage in diesem Zusammenhang häufig fälschlicherweise von der „Trennung von Infrastruktur und Betrieb“ gesprochen wird. Tatsächlich werden aus systemimmanenten Gründen auch weiterhin die Infrastrukturunternehmen für die Betriebsführung verantwortlich sein. Denn die Aufgabe der Betriebsführung der Eisenbahnen, so wird schon an den zitierten Quellen aus dem 19. Jahrhundert deutlich, besteht in der Lösung des Problems der Zuteilung der Ressource

[4] Gray, Oberservations, 1820, zitiert in [Sch02, S. 28].

[5] Lardner, D.: Railway Economy, London 1851, S. 421-22, zitiert in [SCH02, S. 29]

„Fahrweg“ zu Fahrten von Fahrzeugen und deren Koordination. Die Koordination und Sicherung des Eisenbahnbetriebs auf einer Infrastruktur kann wegen des „zuteilenden Charakters“ dieser Aufgabe nur von einem EIU und nicht von einem oder mehreren darauf verkehrenden EVU geleistet werden. So werden LARDNERs Forderungen aus dem Jahre 1851 nach einer „einheitlichen Leitung“ und einer „Zusammenfassung des gesamten Fuhrbetriebes“ auch heute noch ihrem Grundsatz nach erfüllt, denn die an der Prozessebene relevanten Steuerungs- und Leiteinrichtungen heutiger Eisenbahnen, wie z.B. Stellwerke und Betriebszentralen, sind Einrichtungen der EIU und werden von ihnen betrieben. Dies gilt auch für die geforderte Abstimmung von Fahrzeugbewegungen („aufeinander abgestimmte Bewegungen“), die ihre Entsprechung heute z.B. in der Aufstellung von Fahrplänen und in, zwar kurzfristigen, aber ihrer Natur nach abgestimmten Dispositionsentscheidungen findet.[6]

2.2.2 Einfluss auf die Sicherheit

Die Sicherheit moderner Eisenbahnen wird in einem erheblichen Maße durch die Betriebsverfahren beeinflusst. Unfälle, deren Ursachen im Bereich der Fahrzeuge und der Fahrweginfrastruktur liegen, haben schon seit langer Zeit einen nur geringen Anteil am Unfallgeschehen. Beispielsweise gibt POTTGIEßER in [POT88, S. 13] Ergebnisse einer Untersuchung zum Thema *Mensch und Betriebssicherheit* aus dem Jahre 1975 wieder, nach denen nur 11% der Bahnbetriebsunfälle durch Mängel an Fahrzeugen und Bahnanlagen verursacht wurden, dagegen aber *„68,1% der Bahnbetriebsunfälle auf falsche Handhabung des Dienstes und auf Verstöße gegen Sicherheitsbestimmungen zurückzuführen waren“*. Pottgießer setzt deshalb bei seinen Betrachtungen zur Sicherheitsstrategie der Eisenbahn *„die sachgemäße und reelle Ausführung und Unterhaltung von Wegen und Fahrzeugen als selbstverständlich“* voraus und rückt *„das Regeln und Steuern des Mensch-Maschine-Systems Eisenbahn“* und damit die Betriebsverfahren als wesentliche Quelle von Unfallursachen in den Blickpunkt. Es kommt zugleich zum Ausdruck, dass die „Hardware“ der Eisenbahn, d.h. die reinen technischen Einrichtungen, in einer Art und Weise entwickelt, gefertigt und gewartet werden können, die während des Betriebs ein hohes technisches Sicherheitsniveau gewährleistet. Dies gilt auch für die innerhalb der Betriebsverfahren herangezogenen „technischen Mittel“. BRABAND beispielsweise führt *„glaubwürdige Schätzungen“* an, die den Beitrag des Versagens von „Signalisierungs- und ähnlichen Systemen“ am Unfallgeschehen *„deutlich unter 1%“* sehen [BRA08, S. 27]. Gemeint ist das gefährliche technische Versagen, welches direkt zu einem Unfall führen kann.

[6] Der Verbund von Fahrweginfrastruktur und der Betriebsführung der Eisenbahnen findet bis heute auch in der Zuordnung der Eisenbahnbetriebslehre zu den klassischen Ingenieursstudiengängen seinen Niederschlag: Neben dem Bahnbau gehört auch die Betriebstechnik der Eisenbahn zu den Grundlagenfächern des Bauingenieurwesens. In der Lehre des eher fahrzeugaffinen Maschinenbaus besitzt sie keine vergleichbare Bedeutung.

Die Asymmetrie zwischen den geringen Ursachenanteilen der Fahrzeuge und des Fahrwegs einerseits und den großen Anteilen der Betriebsverfahren andererseits ergibt sich prinzipiell aus der Wahlmöglichkeit zwischen technischen und menschlichen Funktionsträgern. Die Möglichkeit, zwischen Funktionsträgern zu wählen, ist bei den drei Systemelementen sehr unterschiedlich. Mit Fahrzeugen und Fahrwegen werden überwiegend Funktionen ausgeführt, die nur durch technische Systeme realisiert werden können. Bei Betriebsverfahren hingegen kann im Prinzip zwischen verschiedenen Funktionsrealisierungen mit unterschiedlichen Technisierungsgraden gewählt werden. Deshalb kann bei der Gestaltung von Betriebsverfahren der gegenüber sicherheitsrelevanten technischen Systemen fehlerhaftere Mensch nicht nur unmittelbar im Rahmen von Regelhandlungen eingesetzt werden, sondern auch im Falle des Ausfalls eines technischen Systems relativ kurzfristig mit einer Ersatzhandlung die Ausführung der entsprechenden Funktion übernehmen. Fällt beispielsweise eine technische Einrichtung zur Freiprüfung eines Gleises aus, so kann das Freisein ersatzweise durch den Menschen geprüft werden. Bei Fahrzeugen und Fahrwegen hingegen können so grundlegende Funktionen wie z.B. jene von Zughaken, Motor, Bremse und Schiene nicht durch menschliche Funktionsträger ersetzt werden. Deshalb ist die Aufgabe des Menschen im Falle eines hemmenden Funktionsversagens bei Fahrzeugen oder Fahrweg auf die Bereitstellung eines technischen Ersatzsystems beschränkt und nicht auf die Übernahme der Funktionsausführung.

Wegen der Substituierbarkeit durch menschliche Funktionsträger spielt die Verfügbarkeit der entsprechenden technischen Mittel für die Sicherheit der Betriebsverfahren eine besondere Rolle. Es konnte beispielsweise anhand der Risikoanalyse FunkFahrBetrieb (FFB) gezeigt werden, dass das zunächst zwar ungefährliche hemmende technische Versagen einer technischen Einrichtung für die Betriebsabwicklung wegen seiner Substitution in der Rückfallebene indirekt bei einem häufigen hemmenden Versagen in einem wesentlich größeren Maße zum Risiko beiträgt als sein sehr seltenes gefährliches Versagen; s.a. [BRA05, S. 81].

Auch wenn für moderne Eisenbahnsysteme wegen der unterschiedlichen Betriebsverfahren und deren verschiedenen Technisierungsgraden bezüglich der Verteilung der Unfallursachen keine allgemeingültigen Zahlen angegeben werden können, so darf zusammenfassend festgestellt werden, dass der überwiegende Anteil der Unfallursachen im Bereich der Betriebsverfahren liegt und durch fehlerhafte Regelhandlungen sowie durch die Verfügbarkeit der eingesetzten Technik und die im Falle der Nichtverfügbarkeit in der Rückfallebene erforderlichen Ersatzhandlungen dominiert wird (Bild 6).

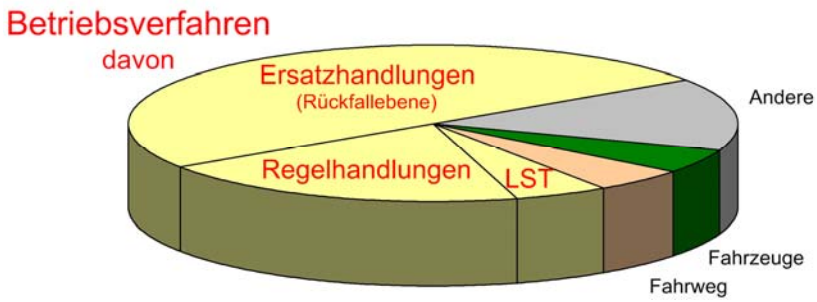


Bild 6: Darstellung prinzipieller Größenordnungen der Anteile an Unfallursachen

Alle technischen Mittel des Systems Eisenbahn tragen mit ihrem gefährlichen Versagen i.d.R. nur zu einem kleinen Teil zum Gesamtrisiko bei. Sollen zukünftig nennenswerte Verbesserungen bei der Sicherheit der Eisenbahnen erzielt werden, wird dies durch Maßnahmen im Bereich der Betriebsverfahren erreicht werden müssen.

Damit können im Hinblick auf die Sicherheit für die Neugestaltung von Betriebsverfahren folgende vier miteinander verknüpfte Anforderungen definiert werden:

- Verbessern der Handlungssicherheit bei Regelhandlungen,
- Ersetzen von Regelhandlungen durch technische Systeme,
- Erhöhen der Verfügbarkeit der eingesetzten technischen Systeme zur Vermeidung von Ersatzhandlungen,
- Verbessern der Handlungssicherheit bei Ersatzhandlungen in der Rückfallebene.

2.3 Dokumentation des betrieblichen Systemwissens

Wie in den vorstehenden Abschnitten dargelegt worden ist, sind die Betriebsverfahren von zentraler Bedeutung für die Durchführung und die Sicherheit des Eisenbahnbetriebs. Entscheidend für die sichere Durchführung des Betriebs ist ein umfassendes Systemwissen der an der Betriebsdurchführung beteiligten Akteure. Dementsprechend detailliert wird das benötigte Systemwissen in betrieblichen Regelwerken aufbereitet und dokumentiert. Dies geschieht z.B. in den Fahrdienstvorschriften der Bahnen.

Die Variabilität bei der Ausgestaltung mit betrieblichen Regeln und technischen Hilfsmitteln führt zu einer großen Zahl zwar detaillierter, aber eben auch verschiedener Dokumentationen und Beschreibungen. Aus der Sicht der einzelnen Bahnen ist das unternehmerisch naheliegend. Es ist deshalb nachvollziehbar, dass es bislang nur wenig eisenbahnspezifische Fachliteratur gibt, die das Systemwissen in einer von unternehmensspezifischen und nationalen Sichtweisen abstrahierenden Darstellung zusammenfasst und dokumentiert. Auch gibt es bislang keine allgemeine funktionale Beschreibung des Systems Eisenbahn. So bezeichnet BEPPERLING diesbezügliche Bemühungen für eine EN 50127 (Railway Applications – guide to the specification of a guided transport system), als „gescheitert“ [BEP08, S.44]. Diese Situation trifft aber nicht nur auf die interne Ausbildung bei den

Eisenbahnen, sondern auch auf die Eisenbahnlehre an den Hochschulen zu, die i.d.R. traditionell an den jeweils national geprägten betrieblichen Grundsätzen ausgerichtet sind. PACHL z.B. variiert Vorlesungen zu ein und demselben Themenkreis entsprechend der national ausgerichteten Bedürfnisse seiner Hörer[7].

2.4 Generisches Referenzsystem

Mit der zunehmenden Globalisierung der eisenbahnspezifischen Märkte erwächst das Bedürfnis nach einer entsprechend übergreifenden Aufbereitung des eisenbahnspezifischen Systemwissens. Dies betrifft nicht nur die grenzüberschreitenden Verkehre, sondern auch die Vorgabe einheitlicher Sicherheitsziele. Insbesondere für die Vorgabe der Sicherheitsziele ist eine einheitliche Bezugsbasis erforderlich, um die Ziele definieren und vorgegeben zu können. In dieser Arbeit werden Grundlagen für ein generisches Referenzsystem für Betriebsverfahren erarbeitet, die der Schaffung einer einheitlichen funktionalen Bezugsbasis dienen.

Begriffsbildung

Unter dem Begriff *Generisches Referenzsystem* wird in dieser Arbeit ein imaginäres System generischer Funktionen verstanden. Die darin enthaltenen Funktionen werden unabhängig von technischen oder regelbasierten Realisierungen und Architekturen beschrieben. Damit ist es nicht möglich, im gegenständlichen Sinne Subsysteme oder Systemkomponenten anzugeben.

Ein generisches Referenzsystem für Betriebsverfahren muss die grundlegenden funktionalen Zusammenhänge des Systems Eisenbahn unabhängig von unternehmerischen und nationalen Betriebsgrundsätzen abbilden. Weil, wie zu Beginn des Abschnittes 2.2 erläutert worden ist, die Betriebsgrundsätze ihren unmittelbaren Niederschlag in den auf betrieblichen Regeln und technischen Hilfsmittel bestehenden Betriebsverfahren finden, muss eine generische Referenz ferner unabhängig von den angewandten Regeln und der eingesetzten Technik sein. Damit darf eine generische Referenz, die das grundsätzliche Funktionieren des Systems Eisenbahn abbilden soll, nur auf der Basis in jeglicher Hinsicht abstrahierender, d.h. realisierungsunabhängiger betrieblicher Funktionen und Wirkungszusammenhängen gebildet werden (Bild 7).

[7] Mdl. Information gegenüber dem Autor dieser Arbeit

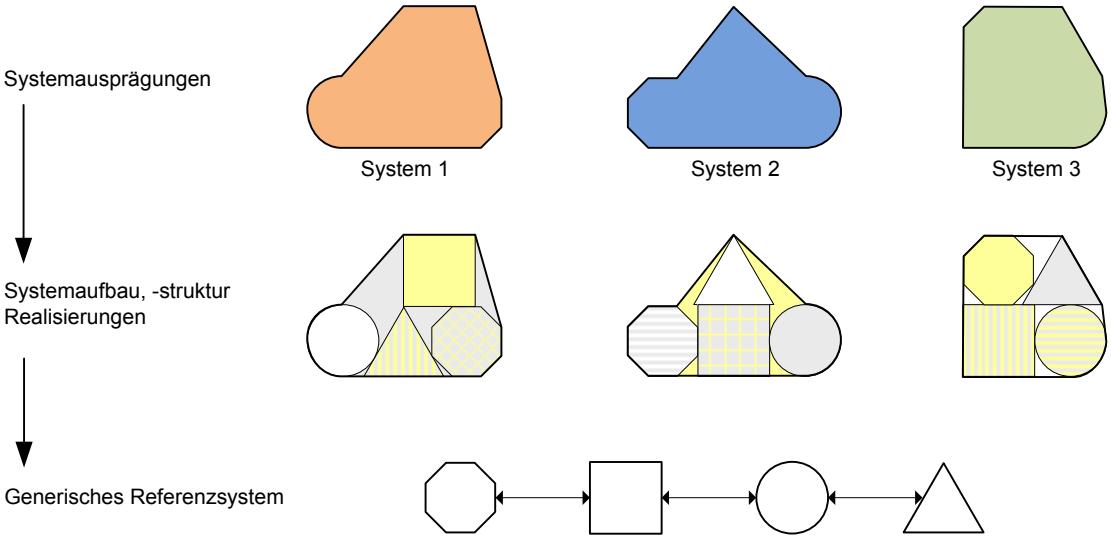


Bild 7: Generisches Referenzsystem auf Basis betrieblicher Funktionen und Wirkungszuammenhänge

Weiteres Vorgehen

Das Bestreben, bestimmte Systeme und Verfahren zumindest in einem gewissen Maße zu abstrahieren und realisierungsunabhängig zu beschreiben, ist im Eisenbahnwesen nicht neu. In verschiedenen Risikoanalysen sind beispielweise zu entwickelnde technische Systeme in Lastenheften spezifiziert, ihre Gefährdungen auf einer als generisch definierten Basis identifiziert und in Gefährdungslisten dokumentiert worden. Ihre Eignung für ein generisches Referenzsystem für Betriebsverfahren werden im Kapitel 3 analysiert.

3 Analyse betriebsverfahrensaffiner Funktions- und Gefährdungslisten

In diesem Kapitel werden vorliegende Funktions- und Gefährdungslisten sowie weitere Ansätze dahingehend analysiert, inwieweit sie für das Schaffen einer generischen Referenz für Betriebsverfahren als Ausgangsbasis herangezogen oder anderweitig, z.B. zum „Mappen“ der Ergebnisse eingebunden werden können. Dazu wird zunächst eine einheitliche Analysebasis geschaffen.

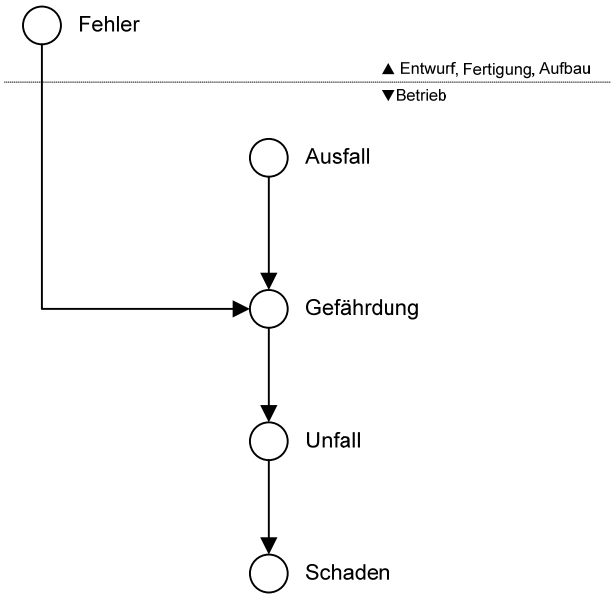
3.1 Bilden einer einheitlichen Analysebasis

Um die im Rahmen verschiedener Projekte und aus unterschiedlichen Motivationen heraus entstandenen Funktions- und Gefährdungslisten vergleichen zu können, muss für die Analyse dieser Listen zunächst eine einheitliche Analyse- und Begriffsbasis geschaffen werden. Sie orientiert sich im Wesentlichen an den in den CENELEC-Normen niedergelegten Prinzipien, die sich als EN 50126 und 50129 etabliert haben.[8]

3.1.1 Wirkungskette

Mit der Wirkungskette wird der grundsätzliche Zusammenhang von Fehler, Ausfall, Gefährdung, Unfall und Schaden dargestellt (Bild 8). Er besagt, dass sich ein Fehler, der bei der Planung, der Realisierung, dem Entwurf oder der Fertigung eines Funktionsträgers „begangen“ wurde, während des Betriebs eines Systems gefährlich auswirken kann. Dies gilt ebenso für den Ausfall eines Funktionsträgers während des Betriebs. Die durch Fehler und Ausfälle hervorgerufenen Gefährdungen können zu Unfällen mit einer Schadensfolge führen.

[8] Bei der Einbeziehung dieser Normen ist zu beachten, dass ein wesentliches Ziel, das mit diesen Normen verfolgt wird, in dem korrekten und effizienten Durchführen von Sicherheitsanalysen einschließlich der Zuscheidung der Betreiber- und Herstellerverantwortlichkeiten und der Definition einer entsprechenden Schnittstelle zwischen den Verantwortungsbereichen liegt. Es wird mit diesen Normen nicht vorrangig das Ziel verfolgt, die Betriebsverfahren des Systems Eisenbahn detailliert in allen ihren Wirkungszusammenhängen beschreiben zu wollen, sondern nur jene Zusammenhänge und Mechanismen zu berücksichtigen, von denen ein sicherheitsrelevanter Einfluss erwartet wird, der bei der Entwicklung technischer Systeme und ihrer Komponenten von den Herstellern zu berücksichtigen ist. Dementsprechend sind die Begriffswelt der Normen, das methodische Vorgehen sowie die Vorgaben hinsichtlich der Beschreibung des Systems Eisenbahn auf die Sicherheitsanalysen fokussiert. Es ist deshalb darauf zu achten, dass Funktionalitäten von Betriebsverfahren, die nicht technisch realisiert werden können oder sollen, dennoch in die Beschreibung eines generischen Referenzsystems einbezogen werden.



Nichterfüllung einer Forderung (Planungs-, Realisierungs-, Entwurfs-, Fertigungsfehler). [DIN 40041]

Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung. [DIN 40041]

Bedingung, die zu einem Unfall führen kann. [EN 50129]

Ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder von Umweltschäden. [EN 50129]

Folge eines Unfalls; s. Unfall

Bild 8: Wirkungskette nach [FP90] mit ergänzenden Definitionen

Der mit der Wirkungskette dargestellte Zusammenhang ist elementar. Er ist die Basis für die in den aktuellen Normen EN 50126 und EN 50129 niedergelegten Verfahren zur Führung von Risikoanalysen und Sicherheitsnachweisen. Der Begriff ist in älterer Literatur ebenso zu finden wie in aktuellen universitären Lehrmaterialien; vgl. a. [FP90, S. 65][9], [PAC08-1].

Erweiterung der Begriffsdefinition

Die Zuordnung des Fehlers in der Wirkungskette zur vorbetrieblichen Lebenszyklusphase „Entwurf, Fertigung, Aufbau“ und des Ausfalls zur Betriebsphase deckt sich mit den Definitionen der DIN 40041. Allerdings ist die Formulierung der Definitionen in der DIN sprachlich in ähnlicher Weise an technischen Systemen orientiert wie die Darstellung und Erläuterung der Wirkungskette in [FP90, S. 65]. Im Hinblick auf die heute übliche realisierungs**un**abhängige Betrachtungsebene, die sowohl technischen als auch verfahrensbasierten Funktionsrealisierungen gerecht werden soll, und dem Fokus auf Betriebsverfahren wird die Definition der Begriffe „Fehler“ und „Ausfall“ wie folgt erweitert: Systematische Fehler umfassen „Technikfehler“ sowie „Regelwerksfehler“. Als „zufällige Fehler“ werden sowohl „Technikausfälle“ als auch „Fehlhandlungen“ verstanden (s.a. Bild 9 und Tabelle 1).

[9] Die von FRICKE und PIERICK in [FP90] genutzte Bezeichnung Ereigniskette sollte wegen der Verwechslungsgefahr mit dem heute auch im Zusammenhang mit „Sicherheit“ und „Risiko“ genutzten Begriff Ereignisbaum nicht verwendet werden (s.a. 3.1.3). In dieser Arbeit wird nachfolgend ausschließlich der Begriff „Wirkungskette“ verwendet.

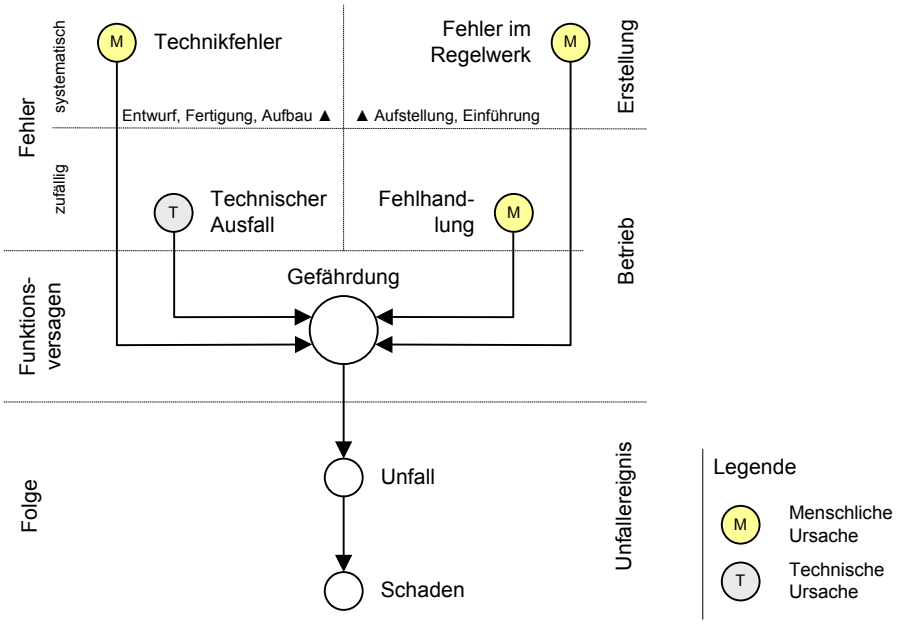


Bild 9: Mögliche Fehlerarten und Ereignisverkettung[10]

Tabelle 1: Erweiterung der Definitionen für „Ausfall“ und „Fehler“

[DIN 40041]		**Erweiterung der Definition**	
Fehler	Nichterfüllung einer Forderung (Planungs-, Realisierungs-, Entwurfs-, Fertigungsfehler).	Technik-fehler	Systematischer Fehler, der beim Entwurf, der Fertigung oder dem Aufbau eines technischen Systems vom Menschen „begangen“ worden ist.
		Regelwerks-fehler	Systematischer Fehler, der bei der Aufstellung oder der Einführung eines betrieblichen Regelwerks vom Menschen „begangen“ worden ist.
Ausfall	Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung.	Technik-ausfall	Zufälliger Fehler eines technischen Systems, das bei seiner Inbetriebnahme als fehlerfrei gelten durfte.
		Fehl-handlung	Zufälliger Fehler eines Menschen bei der Ausführung einer betrieblichen Regel, die bei ihrer Einführung als fehlerfrei gelten durfte. Gilt auch für „Ausfall“ des Menschen bei der Regelausführung z.B. durch Tod, Ohnmacht.

Werden im Rahmen dieser Arbeit die Begriffe „Fehler“ und „Ausfall“ verwendet, so sind sie als Oberbegriffe entsprechend der Tabelle 1 zu verstehen.

[10] Anmerkung: Das Bild dient der Definition von Begriffen. Die „Verfügbarkeitsproblematik“, die sich daraus ergibt, dass ein hemmendes Versagen der Technik durch Handlungen des Menschen substituiert wird und es dabei zu einem gefährlichen Versagen kommt, wird hier nicht dargestellt.

3.1.2 Wirkungskettenorientierte Darstellung der Risikodefinition

Sicherheit ist nach EN 50129 das „Freisein von nicht akzeptierbaren[11] Risiken eines Schadens“. Als Risiko wird in derselben Norm die „Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses“ definiert. Die Folgen einer Gefährdung sind laut Wirkungskette der Unfall und der Schaden. Da es ohne Unfall keinen Schaden geben kann, aber auch ein Unfall ohne Schaden kein Unfall ist, bleibt in beiden Fällen die Gefährdung folgenlos. Ebenfalls nach EN 50129 gilt, dass einer Gefährdung ein Unfall folgen kann, aber nicht muss. Insofern ist für die Ermittlung des Risikos letztlich das Produkt aus der Wahrscheinlichkeit des Unfalleintritts und dem Schadensausmaß interessant. Dies entspricht auch der Risiko-Definition der IEC 61508 [IEC 61508-4]. Es ergibt sich die an der Wirkungskette orientierte Darstellung der Risiko-Definition (Bild 10).

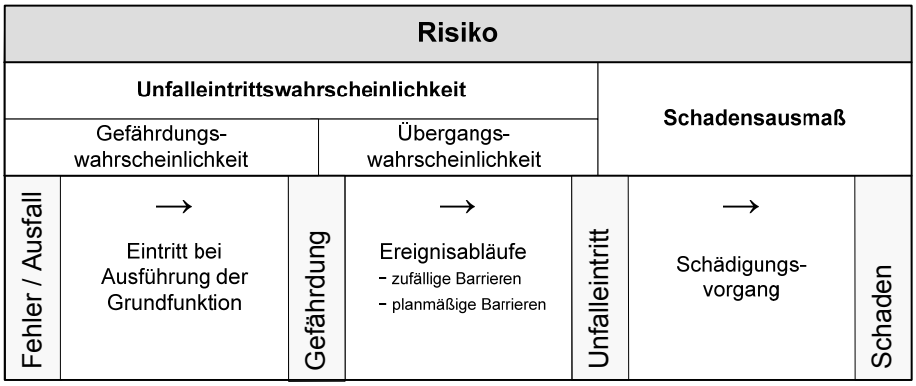


Bild 10: Wirkungskettenorientierte Darstellung der Risikodefinition

Das Risiko ist das Produkt aus Unfalleintrittswahrscheinlichkeit und Schadensausmaß. Die Unfalleintrittswahrscheinlichkeit selbst setzt sich aus der Gefährdungswahrscheinlichkeit und einer Wahrscheinlichkeit zusammen, mit der eine eingetretene Gefährdung in einen Unfall übergeht. Die Gefährdungswahrscheinlichkeit wird durch die Häufigkeit des Eintretens ihrer Ursachen, d.h. ihrer Fehler und Ausfälle bestimmt. Die Übergangswahrscheinlichkeit wird durch die der Gefährdung folgenden Ereignisabläufe und der Wirksamkeit der darin enthaltenen zufälligen und planmäßigen unfallvermeidenden Barrieren beeinflusst. Mit dem

[11] Anmerkung zur aktuellen Diskussion des Begriffs „akzeptierbares Risiko“: Die in Deutschland bislang übliche Praxis, für den Nachweis einer mindestens gleichen Sicherheit, einen aus Unfallstatistiken abgeleiteten vorhandenen Risikowert als „akzeptiertes Risiko“ zu interpretieren und vorzugeben, wird nach Angaben des Eisenbahn-Bundesamtes, die dem Autor dieser Arbeit aus mündlichen Quellen bekannt geworden sind, in Juristenkreisen offenbar zunehmend kritisiert. Die Argumentation der Kritiker begründet sich darin, dass jeder in der Statistik erfasste Unfall mit der Folge eines Personenschadens zumindest staatsanwaltschaftliche Ermittlungen zur Folge gehabt habe und somit für sich genommen ein nicht akzeptiertes Ereignis. Daraus wird die Schlussfolgerung gezogen, dass eine Summe nicht akzeptierter Ereignisse nicht als akzeptierbares Risiko bezeichnet werden dürfe.

Unfalleintritt entsteht ein Schaden, dessen Ausmaß vom Verlauf des Schädigungsvorgangs beeinflusst wird. Der Schädigungsvorgang ist schwer zu bestimmen und wird deshalb bei Risikobetrachtungen i.d.R. nicht analysiert. Vielmehr wird auf empirische, statistisch gestützte Erfahrungen zurückgegriffen, um unter Berücksichtigung betrieblicher Randbedingungen den Zusammenhang zwischen Unfallart und Schadensausmaß zu beschreiben.

Berücksichtigung des Schädigungsvorgangs

Da der Fokus dieser Arbeit nicht auf Methoden zur expliziten Risikoermittlung gerichtet ist, sondern im wesentlichen das Ziel verfolgt, durch Betriebsverfahren realisierte Funktionen sowie deren Wirkungsweisen und -beziehungen im Sinne der Wirkungskette zu beschreiben, wird auch der jedem Unfall innewohnende Schädigungsvorgang als Bestandteil des Risikomodells dargestellt. Dies ist auch deshalb wichtig, weil das System Eisenbahn durchaus Einrichtungen kennt, mit denen Funktionen realisiert werden, die ausschließlich der Reduzierung der Folgen eines bereits eingetretenen Unfalls dienen. Ein zwar nicht zum Bereich der Betriebsverfahren gehörendes, aber häufig anzutreffendes Beispiel für derartige Einrichtungen sind Führungsschienen, die die Funktion besitzen, entgleiste Fahrzeuge möglichst dicht am Gleis zu führen und auf diese Weise die Wahrscheinlichkeit eines Absturzes z.B. im Bereich von Brücken zu reduzieren. Die Funktion wird im ungefährdeten Zustand für die Abwicklung des Betriebs nicht benötigt. Vergleichbares gilt für die Notbremsüberbrückung.

Auch aus Sicht zu gestaltender Betriebsverfahren ist eine detaillierte Betrachtung und Kenntnis der bis zum Schädigungsvorgang reichenden Wirkungszusammenhänge interessant[12]. Während es sich z.B. bei Kollisionen um zeitlich und räumlich sehr kurze Unfall- und Schädigungsvorgänge handelt, werden insbesondere in Güterzügen entgleiste Wagen – das Engleisen ist bereits der Unfalleintritt! – oftmals mehrere Kilometer weit mitgezogen, ohne dass ein großer Schaden eintritt. Erst bei der ersten im weiteren Streckenverlauf liegenden Weiche eskalieren die Schadensausmaße wegen der dabei eintretenden Zerstörung der

[12] Es besteht kein Widerspruch zu Methoden, wie z.B. das Verfahren Risikograph [VDV 331] und der Ansatz BP Risk [BEP08], mit deren Hilfe im Rahmen von Sicherheitsnachweisen der Aufwand für die Abbildung von Ereignisbäumen und die Berechnung von Risikoreduktionsfaktoren reduziert werden soll. Vielmehr werden für umfassende generische Systembetrachtungen nicht nur detaillierte Kenntnisse über die planmäßigen, sondern auch über die nach dem Versagensfall auftretenden prinzipiellen Wirkungszusammenhänge benötigt. Letztere werden in Ereignisbäumen abgebildet.

Weiche und des weiteren Fahrwegs erheblich.[13] In solchen Fällen wäre es, zumindest theoretisch, möglich, Maßnahmen in geeigneter Weise funktional zu integrieren, die eine Detektion der Entgleisung in einer frühen Phase des Unfallablaufs ermöglichen und auf diese Weise zu einer Risikoreduktion führen würden; vgl. a. [HL09].

3.1.3 „Sanduhr“

Die Prozesse zur Analyse der Ursachen und Folgen von Gefährdungen werden i.d.R. mit einer Sanduhr symbolisiert. Sie beruht auf den CENELEC-Normen und in zahlreichen Veröffentlichungen in vielfältiger Darstellung abgebildet.

Das obere Dreieck ist ein Sinnbild für die Analyse der Folgen einer Gefährdung anhand von Ereignisbäumen, das untere ist das Sinnbild für die Analyse der Gefährdungsursachen mit Fehlerbäumen (Bild 11).

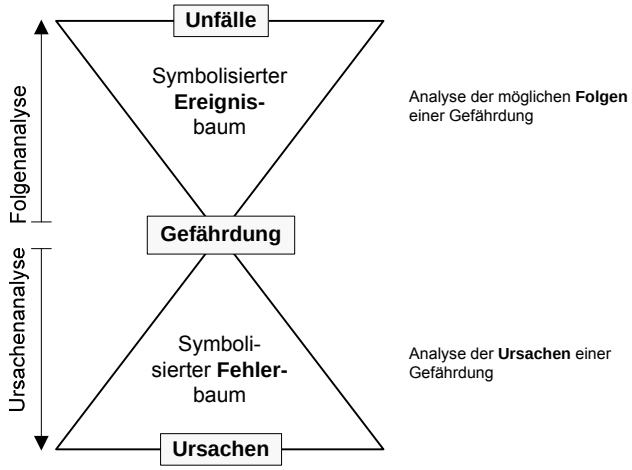


Bild 11: Symbolik der CENELEC-Sanduhr

An der Schnittstelle beider Dreiecke werden für ein zu realisierendes System zum einen Gefährdungsraten vorgegeben, die zur Einhaltung eines bestimmten Risikogrenzwertes erforderlich sind und zum anderen wird der Nachweis erbracht, dass die gewählte System-realisierung diese Raten einhält. Während die Wirkungskette (Bild 8) auf die Darstellung der Wirkungszusammenhänge zwischen der Ursache und dem Unfall und dessen Schaden abzielt, wird mit der Sanduhr-Darstellung der Blick auf das methodische Vorgehen bei der

[13] Ein solcher Wirkmechanismus lag auch dem Unfall des ICE 884 am 3. Juni 1998 zugrunde. Mit dem Bruch eins Radreifens, er entspricht einer Entgleisung, begann der Unfall bereits 5,5 km vor der im folgenden Bahnhof liegenden Straßenbrücke. Trotz des defekten Rades fuhr der Zug ohne von innen spürbare Beeinträchtigungen rund 100 Sekunden weiter, bevor der Schädigungsvorgang an der ersten im Fahrweg liegenden Weiche eskalierte [BP01]. So gesehen stellt dieser Unfall weniger durch seinen Wirkmechanismus, sondern mehr wegen seines Schadensausmaßes und der betroffenen Zuggattung eine Besonderheit dar.

Risikobeurteilung gelenkt. Diese Darstellung stimmt, wie im Abschnitt 3.1.4 gezeigt wird, mit den Wirkungszusammenhängen der Wirkungskette und mit der Definition der Risikobegriffe überein.

3.1.4 Vergleichende Gegenüberstellung

Die wirkungskettenorientierte Darstellung der Risikodefinition und die im Application Guide CLC/TR 50126-2 enthaltene detaillierte Darstellung der CENELEC-Sanduhr werden im Bild 12 gegenübergestellt. Die Gemeinsamkeiten und Unterschiede werden in der Tabelle 2 erläutert. Ziel ist das Überführen in eine gemeinsame Darstellung, die als einheitliche Bezugsbasis für die Analysen herangezogen werden kann, die in den Abschnitten 3.2 bis 3.3 durchgeführt werden.

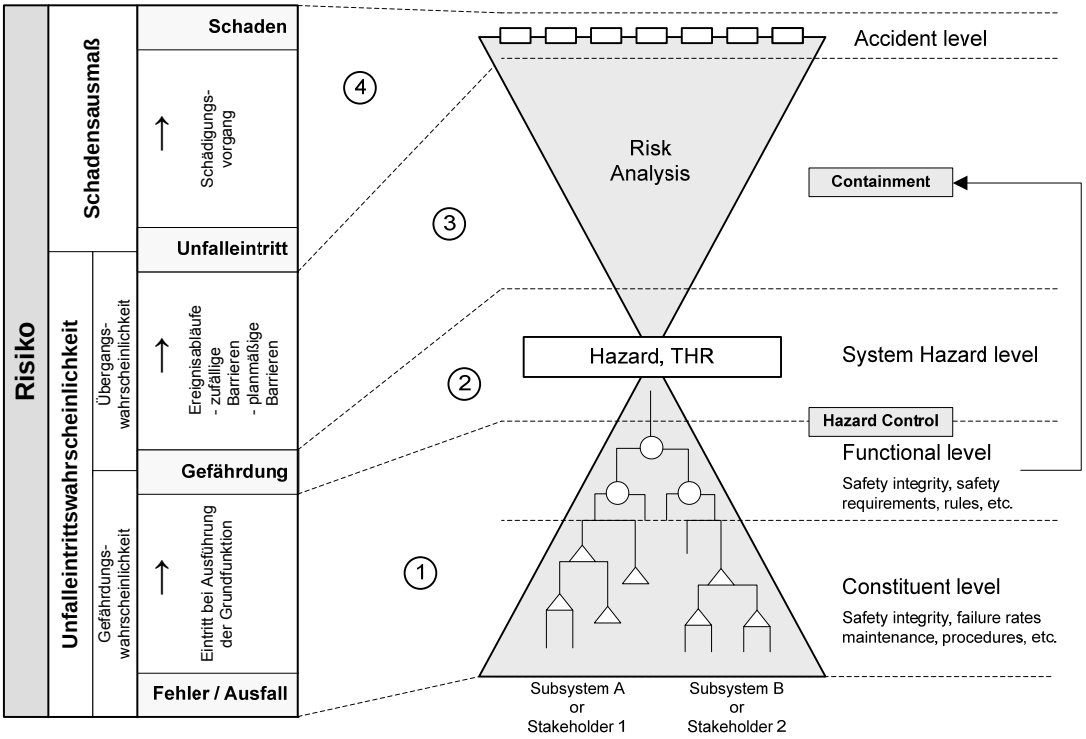


Bild 12: Vergleich Risiko-Definition (Bild 10) mit der Sanduhr nach CLC/TR 50126-2

Tabelle 2: Vergleich von Risiko-Definition und „Sanduhr“

①	In der Risiko-Definition wird dargestellt, dass Fehler und Ausfälle für das Eintreten einer Gefährdung ursächlich sind. Sie führen mit einer bestimmten Wahrscheinlichkeit bei Ausführung der davon betroffenen Funktion zu einer Gefährdung. Mit dem in der „Sanduhr“ angedeuteten Fehlerbaum wird erläutert, dass die Wahrscheinlichkeit des Gefährdungseintritts nicht nur durch das Auftreten von Fehlern und Ausfällen, sondern auch vom Systemaufbau, d.h. von der Verknüpfung der technischen und menschlichen Komponenten, abhängig ist. Die Aufteilung eines Systems in Komponenten wird durch die Ebene „Consituent level“ und deren Zusammenwirken durch die Ebene „Functional level“ dargestellt.

②	In beiden Darstellungen bildet die Gefährdung (Hazard) den Übergang vom ungefährdeten in den gefährdeten Betriebsablauf.
③	Zwischen der Gefährdungsebene und der Unfallebene sind die Ereignisabläufe angeordnet. In der Risikodefinition werden sie namentlich erwähnt, in der „Sanduhr" durch das obere Dreieck symbolisiert. Der Begriff „Risikoanalyse" drückt keinen Wirkungszusammenhang aus, sondern steht hier für einen Arbeitsschritt im Rahmen eines Sicherheitsanalyseprozesses. In beiden Darstellungen sind Faktoren zu finden, die die Entwicklung der Ereignisabläufe beeinflussen. In der Risikodefinition sind dies die „zufälligen" und die „planmäßigen Barrieren". Unter dem Ausdruck „Containment", zu deutsch Beherrschung, Eindämmung und Eingrenzung, sind Maßnahmen zu verstehen, die, bereits in die Systemarchitektur implementiert, dazu dienen sollen, eine eingetretene Gefährdung so einzudämmen, dass die Übergangswahrscheinlichkeit zu einem Unfall gesenkt wird. Dies entspricht dem Gedanken der „planmäßigen Barrieren".
④	Während in der „Sanduhr" die Unfall-Ebene nur andeutungsweise abgebildet wird, wird in der Risiko-Definition deutlicher auf die Wirkungszusammenhänge dieser Ebene eingegangen. Es liegt jedoch kein inhaltlicher Unterschied vor. Die Unterschiede in der Beschreibungstiefe finden ihre Erklärung in den unterschiedlichen Einsatzzwecken der Darstellungen: Mit der Risikodefinition werden Wirkungszusammenhänge zwischen den das Risiko bestimmenden Faktoren erläutert. Dazu gehören auch jene, die nach Eintritt des Unfalls einen Einfluss auf das Schadensausmaß haben. Die „Sanduhr" hingegen dient der Beschreibung eines methodischen Vorgehens zur Risikobeurteilung und zum Nachweis der Sicherheit. Weil die Wirkungszusammenhänge der Unfall-Ebene i.d.R. vielgestaltig sind, können sie nicht als risikoanalysetaugliches Modell abgebildet werden. Der Zusammenhang zwischen Unfall und Schadensausmaß wird deshalb meist empirisch, d.h. ohne Betrachtung des Schädigungsvorgangs, beschrieben.

Fazit

Sowohl die „Sanduhr" als auch die Risiko-Definition decken den Bereich der Wirkungskette (Bild 8) ab. Alle Elemente der Wirkungskette, d.h. Fehler, Ausfall, Gefährdung, Unfall und Schaden, werden, wenn auch mit unterschiedlicher Zielsetzung, abgebildet bzw. angedeutet. Der Vergleich der „Sanduhr" mit der an die Wirkungskette angelehnten Risiko-Definition hat gezeigt, dass sie im unteren Dreieck wesentlich detaillierter die Wirkungszusammenhänge als im oberen abbildet. Dagegen werden die Wirkungszusammenhänge im Bereich des oberen Dreiecks durch die Risiko-Definition ausführlicher dargestellt.

3.1.5 Modifizierte Sanduhr

Um innerhalb dieser Abhandlung bei den weiteren Arbeitsschritten auf eine einheitliche Darstellung zurückgreifen zu können, die die Wirkungszusammenhänge wiedergibt, auf den Sicherheitsanalyse-Prozess verweist und den Bezug zum Eisenbahnbetrieb herstellt, wird eine gemeinsame Darstellungsform abgeleitet. Sie orientiert sich an der in der Literatur und den Normen geläufigeren Sanduhr-Darstellung, definiert die Begriffe „Betriebliche Grundfunktion" und „Gefährdung" eindeutig auf die Prozessebene des Eisenbahnbetriebs bezogen und stellt im Bereich des oberen Dreiecks die Zusammenhänge detaillierter dar (Bild 13).

Erläuterung

Die modifizierte Sanduhr wird in der Tabelle 3 anhand der im Bild 13 zur Orientierung angegebenen Ziffern ① bis ⑬ im Detail erläutert.

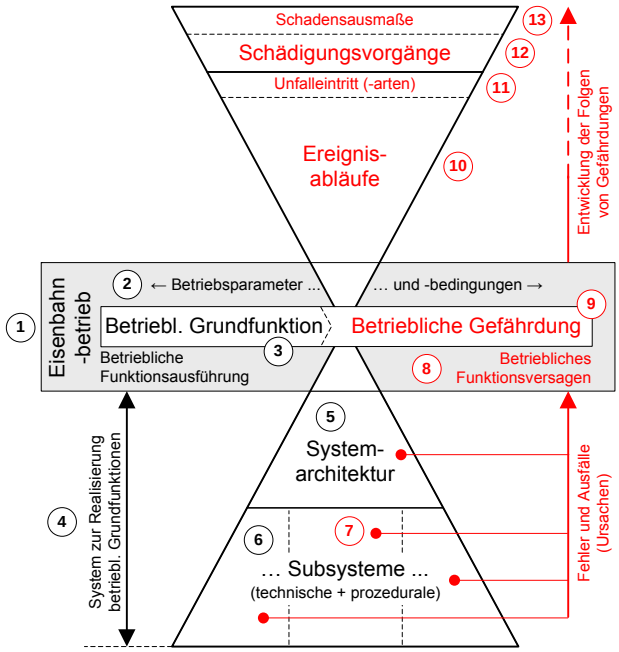


Bild 13: Wirkungskette in modifizierter Sanduhr-Darstellung

Tabelle 3: Erläuterung der modifizierten Sanduhr-Darstellung

①	**Eisenbahnbetrieb** Der Eisenbahnbetrieb dient der Abwicklung von Personen- und Güterverkehren in Fahrzeugen auf einer Fahrweginfrastruktur. Die sichere Durchführung des Eisenbahnbetriebs beruht auf der Beherrschung der mit den Fahrzeugbewegungen einhergehenden physikalischen Gesetzmäßigkeiten, da die kinetische Energie der bewegten Fahrzeuge im Falle von Fehlfunktionen unkontrollierbar werden und zu Schäden führen kann. Der Eisenbahnbetrieb bildet die Bezugsebene für die weiteren Betrachtungen.
②	**Betriebsparameter und -bedingungen** Der Eisenbahnbetrieb ist durch betriebliche Parameter und Situationen, infrastrukturelle Gegebenheiten sowie technische Rand- und Umweltbedingungen gekennzeichnet.
③	**Betriebliche Grundfunktion** Um den Eisenbahnbetrieb sicher durchführen zu können, müssen die dafür erforderlichen Funktionen ausgeführt werden. Betriebliche Grundfunktionen dienen unmittelbar eisenbahnbetrieblichen Zwecken. Sie sind gegenüber den möglichen Realisierungen der Systeme, mit denen sie umgesetzt werden, generisch.

(4)	**System zur Realisierung betrieblicher Grundfunktionen** Die betrieblichen Grundfunktionen werden durch Systeme realisiert, die aus betrieblichen Regeln und technischen Mitteln bestehen. Die Möglichkeiten zur Kombination menschlicher und technischer Träger von Systemfunktionen sind vielfältig und erlauben i.d.R. verschiedene Systemrealisierungen.
(5)	**Systemarchitektur** Die Systemarchitektur ist die erste Realisierungsstufe eines Systems, das der Realisierung betrieblicher Grundfunktionen dienen soll. Auf dieser Stufe wird das Zusammenwirken verschiedener Subsysteme zur Realisierung der betrieblichen Grundfunktionen beschrieben. Auch das Verhalten des Systems bei hemmendem Versagen kann auf dieser Ebene als Rückfallebene festgelegt werden. Von der Gestaltung der Systemarchitektur ist es wiederum abhängig, ob und in welchem Maße sich Fehler und Ausfälle der Komponenten als Versagen des Systems und damit als betriebliches Funktionsversagen (8) auswirken können. Die Systemarchitektur ist eine Konkretisierung der betrieblichen Grundfunktionen, sie kann aber gegenüber den möglichen Realisierungen ihrer Subsysteme generisch sein.
(6)	**Subsysteme** Die Komponenten, aus denen ein System besteht, werden als Subsysteme bezeichnet. Sie können als technische Einrichtungen und als vom Menschen ausgeführte Prozeduren realisiert werden. Prinzipiell können die Subsysteme in weitere Subsysteme gegliedert werden.
(7)	**Fehler und Ausfälle** Sie sind Ursachen des betrieblichen Funktionsversagens.
(8)	**Betriebliches Funktionsversagen** Die in einem realisierten System auftretenden Fehler und Ausfälle wirken sich, sofern sie zu Fehlfunktionen des Systems führen, innerhalb des Eisenbahnbetriebs als betriebliches Funktionsversagen aus, d.h. die für die Durchführung des Eisenbahnbetriebs erwartete Ausführung einer betrieblichen Grundfunktion wird vom realisierten System nicht oder nicht korrekt ausgeführt. Es kommt auf der Ebene des Eisenbahnbetriebs während der Funktionsausführung zu einem Funktionsversagen.
(9)	**Betriebliche Gefährdung** Die Betriebliche Gefährdung ist eine spezielle Ausprägung des betrieblichen Funktionsversagens (8). Sie ist dadurch gekennzeichnet, dass das Versagen einer im Eisenbahnbetrieb ausgeführten betrieblichen Funktion zu einem Unfall führen kann.
(10)	**Ereignisabläufe** Mit dem Eintritt einer Betrieblichen Gefährdung (9) entwickeln sich aus dem laufenden Eisenbahnbetrieb heraus Ereignisabläufe, die zu einem Unfall führen können. Die Ereignisabläufe werden durch die beim Gefährdungseintritt vorliegenden Betriebsparameter und -bedingungen (2) beeinflusst.
(11)	**Unfalleintritt** Die Ereignisabläufe (10), die zu einem Unfall führen, gehen mit dem Unfalleintritt in Schädigungsvorgänge (12) über.

(12)	**Schädigungsvorgänge** Die nach den Ereignisabläufen beim Unfalleintritt noch im System vorhandene kinetische Energie wird in Verformungsenergie umgewandelt. Wie zuvor die Ereignisabläufe werden auch die Schädigungsvorgänge durch die beim Gefährdungseintritt vorliegenden Betriebsparameter und -bedingungen (2) beeinflusst.
(13)	**Schadensausmaß** Das Schadensausmaß ist das Ergebnis der Schädigungsvorgänge. Es drückt die Höhe des entstandenen Schadens aus.

Normierung für die Analysen

In der „modifizierten Sanduhr“ werden die Begriffe „Betriebliche Grundfunktion“ und „Betriebliche Gefährdung“ als auf der Ebene des Eisenbahnbetriebsprozesses liegend definiert. Sie werden als komplementär aufgefasst, d.h. eine „Betriebliche Gefährdung“ ist das Versagen einer „Betrieblichen Grundfunktion“, das zu einem Unfall führen kann.

Die Begriffe „Betriebliche Grundfunktion“ und „Betriebliche Gefährdung“ werden als abstrakte Konstrukte aufgefasst. Damit geht die Vorstellung einher, dass sowohl die betrieblichen Grundfunktionen als auch die entsprechenden Gefährdungen unabhängig von jeglicher Realisierung der Systeme definiert und beschrieben werden. Umgekehrt ausgedrückt: Mit den abstrakt zu formulierenden „Betrieblichen Grundfunktionen“ werden die eisenbahnbetrieblich erforderlichen Zwecke der einzusetzenden Systeme realisierungsunabhängig definiert und beschrieben.

Durch die Betrachtung als abstrakte Konstrukte, d.h. durch eine strikte, auch hinsichtlich jeglicher Systemarchitekturen realisierungsunabhängige Betrachtung, werden die Begriffe „Betriebliche Grundfunktion“ und „Betriebliche Gefährdung“ auf einer oberhalb der jeweiligen Systemarchitektur liegenden Ebene definiert.

Um eine „Betriebliche Grundfunktion“ und die aus ihr abgeleitete „Betriebliche Gefährdung“ im vorstehenden Sinne als „normiert“ zu charakterisieren, muss die betriebliche Funktion folgenden Bedingungen genügen:

- Sie dient der Erfüllung eines für die Durchführung des Eisenbahnbetriebs zwingend erforderlichen Zwecks und
- ihre Definition und Beschreibung sind unabhängig von der Realisierung eines Systems, das diesen Zweck erfüllen soll.

Darstellung in den Analysen

Die ausführliche Darstellung der modifizierten Sanduhr gemäß Bild 13 dient ihrer Erklärung. Sie wird im Rahmen der nachfolgenden Analysen in einem gegenüber dem Bild 13 reduzierten Umfang dargestellt (Bild 14). In diese reduzierte Darstellung werden im Rahmen der Analysen Elemente und Ergebnisse der untersuchten Arbeiten eingetragen, um die Gemeinsamkeiten als auch die Unterschiede zu verdeutlichen.

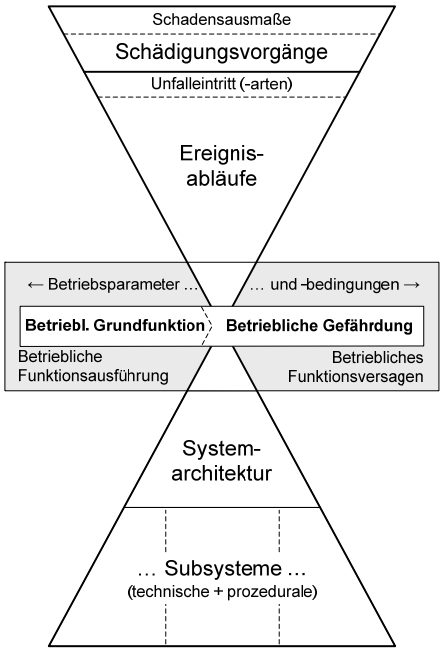


Bild 14: Darstellung der modifizierten Sanduhr in den folgenden Analysen

3.2 Analyse generischer Listen

3.2.1 Generic Hazard List Methodology for Railway Signalling

Der internationale Eisenbahnverband UIC hat im Jahre 2007 im Zusammenhang mit dem Projekt Euro-Interlocking eine generische Gefährdungsliste für Stellwerksfunktionen herausgegeben [UIC07] [14]. Nachfolgend wird analysiert, inwieweit die im Zusammenhang mit diesem Projekt herausgegebenen Dokumente Definitionen für Funktionen und Gefährdungen enthalten, die auch für Betriebsverfahren als generisch angesehen werden können.

Übersicht

Als Ausgangspunkte der Gefährdungsidentifikation werden die Systemarchitektur des Euro-Interlocking und die im Eisenahnwesen möglichen und definierten Unfallarten herangezogen. Als Systemdefinition dienen die Subsysteme und deren Interaktionen, die Informationsflüsse nach sich ziehen. Für jede der möglichen Fehlinformationen, sie werden als Fehlfunk-

[14] Der Begriff „generisch“ wird im Zusammenhang mit Funktions- und insbesondere Gefährdungslisten vielfach verwendet und soll die Allgemeingültigkeit solcher Listen oder Beschreibungen ausdrücken. Allerdings kann eine Liste oder Beschreibung nur innerhalb eines konkreten, d.h. eines definierten Anwendungsgebiets oder einer Anwendungsebene „generisch“ sein. Deshalb ist bei der Verwendung des Begriffes „generisch“ stets zu beachten, dass es sich um einen relativen Begriff handelt.

tionen aufgefasst, wird überprüft, welche der im Eisenbahnwesen möglichen Unfallarten ihr folgen können. Alle sich ergebenden Kombinationen von Fehlfunktionen und möglichen Unfallkonsequenzen werden in der Gefährdungsliste aufgeführt und als Gefährdungen aufgefasst. Im Bild 15 sind die Ausgangpunkte als gelbe Flächen markiert und das Prinzip der Gefährdungsbeschreibungen am Beispiel der Weiche wiedergegeben. Aus den angegebenen drei Gründen und vier möglichen Konsequenzen werden zwölf Kombinationen gebildet, die sämtlich in der UIC-Liste als Gefährdungen eingetragen sind.

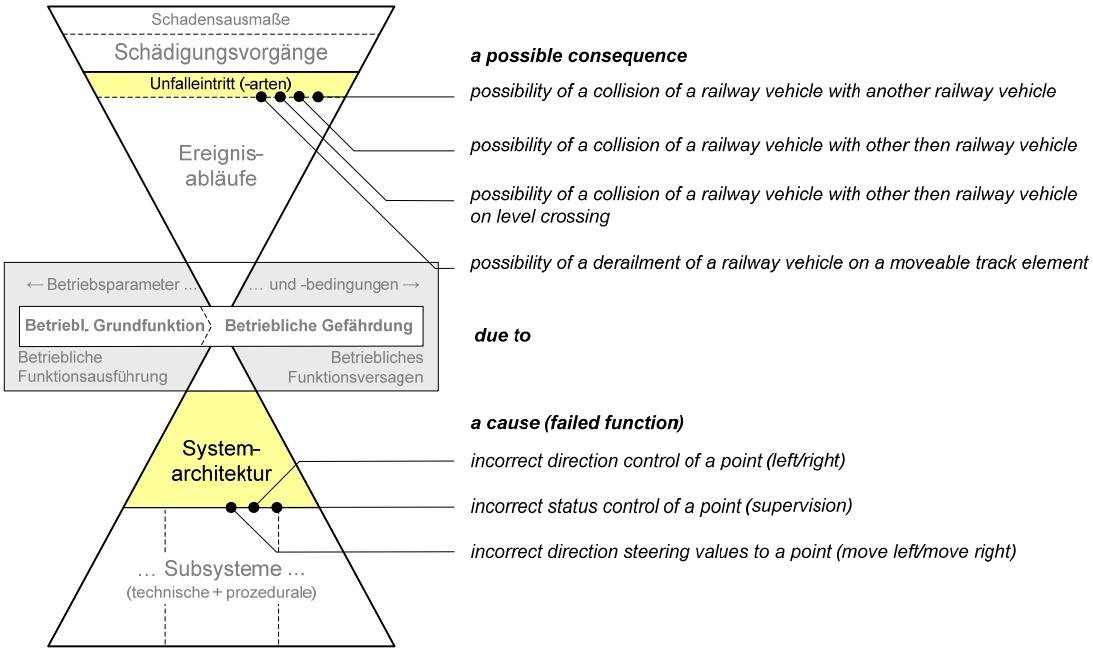


Bild 15: Einordnung der wesentlichen Elemente der UIC-Gefährdungsliste; Beispiel *„Hazards Point Logic / Point“* aus [UIC07]

Erörterung einzelner Aspekte

- Der Betrachtungsraum der UIC-Liste ist ein aus technischen Subsystemen bestehendes generisches Stellwerk. Dieser Betrachtungsraum deckt nur den technisch realisierten Teil der Betriebsverfahren ab. Damit fehlen die durch betriebliche Regeln realisierten Funktionalitäten.
- Die UIC-Liste kann nur bezogen auf eine spätere Realisierung des Stellwerks als generisch angesehen werden. Bezogen auf die Betrachtungsebene Betriebsverfahren ist sie nicht generisch.
- Die Gefährdungsursachen werden auf Basis fehlerhafter Informationsflüsse in einer vorgegebenen Stellwerksarchitektur identifiziert.
- Die in der UIC-Liste aufgeführten Gefährdungen haben keinen unmittelbaren Bezug zu einer betrieblichen Grundfunktion. Es ist zudem fraglich, ob eine Formulierung aus Ursachen und möglichen Folgen als Gefährdung bezeichnet werden sollte.

Ergebnis

Der Schwerpunkt und Wert der UIC-Liste sind in der Definition von Ursachen zu sehen, die sich aus einer bestimmten Stellwerksarchitektur, in diesem Fall dem Euro-Interlocking, ergeben können und von einer späteren Stellwerksrealisierung zu beherrschen sind, damit die mit ihnen angegeben Folgen nicht eintreten. Die UIC-Liste enthält jedoch keine generischen Definitionen für betriebliche Grundfunktionen, die durch Betriebsverfahren realisiert werden. Die in der Liste formulierten „Gefährdungen“ sind lediglich Formulierungen, die aus einer Kombinationen von Gefährdungsursachen mit möglichen Unfallfolgen bestehen. Die Verwendung der UIC-Liste zur Identifikation der mittels Betriebsverfahren zu realisierenden betrieblichen Funktionen und deren möglicher Gefährdungen wird angesichts der der UIC-Liste zugrunde liegenden Zielstellung, ihres auf das Euro-Interlocking beschränkten Betrachtungsraums als auch im Hinblick auf die Methodik ihrer Erstellung als nicht zielführend angesehen.

3.2.2 ROSA – Rail Optimisation Safety Analysis

Das Projekt Rail Optimisation Safety Analysis (ROSA) wird im Rahmen der deutsch-französischen Kooperation in der Verkehrsforschung (DEUFRAKO) bearbeitet. An der Bearbeitung sind neben Forschungseinrichtungen die deutsche DB AG und die französische SNCF als Eisenbahnunternehmen beteiligt. Zu diesem öffentlich geförderten Projekt liegen derzeit noch keine Abschlussberichte oder Fachveröffentlichungen vor. Einige Anhaltspunkte zu dem Projekt sind jedoch einer vom Bundesministerium für Wirtschaft herausgegebenen Broschüre [KPG08] zu entnehmen. Darin werden folgende Ziele angegeben:

- *„im Eisenbahnsystem die Beziehung zwischen Sicherheitszielen und Sicherheitseinrichtungen („Barrieren“, Definition siehe weiter unten) methodisch und logisch zu verbinden*
- *ein computergestütztes Werkzeug zu schaffen*
- *einen Ansatz einer Kosten-Nutzen-Analyse für Sicherheitseinrichtungen zu erarbeiten*
- *die generischen Ergebnisse an Beispielen zu verifizieren*“.

Anhand der im Bild 16 wiedergegeben Grafik und der kursiv gekennzeichneten Zitate aus [KPG08] wird das ROSA-Modell nachfolgend insoweit beschrieben, wie es die zum Zeitpunkt des Entstehens dieser Arbeit vorliegende Veröffentlichungslage zu diesem Projekt erlaubt.

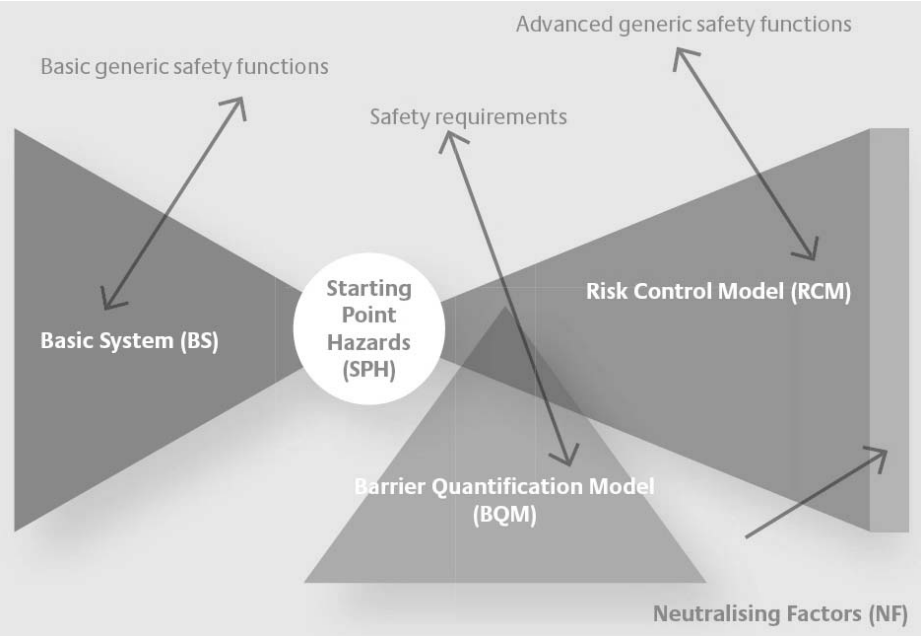


Bild 16: ROSA-Modell [KPG08]

Basic System Model (BS)

„Dies ist ein theoretisches rudimentäres Eisenbahnsystem ohne Sicherheitseinrichtungen, das die prinzipbedingten Eigenschaften des Eisenbahnsystems enthält, [sic!] *sowie zwingend notwendige grundlegende Sicherungseigenschaften, wie z.B. Bremsen im Fahrzeug, Spurführung, Fahrplan mit der Zuordnung von Geschwindigkeit und Fahrzeugort. Es enthält Elemente wie Kreuzungen mit anderen Verkehrsmitteln, Zu- und Abgangsorte von Passagieren und Ladegut, jedoch ohne Sicherungseinrichtungen. Das BS befindet sich im eingeschwungenen Zustand. Die in diesem System aufgrund der nur rudimentären Sicherungseigenschaften entstehenden Fehler werden mit Fehlerbäumen zu Gefährdungen entwickelt und führen zu den Starting Point Hazards SPH.“* [KPG08, S. 11]

Starting Point Hazards (SPH)

„Sie entstehen aus den Fehlerbäumen im BS. Ein Mapping mit den in der DB AG bereits bei Risikoanalysen verwendeten Gefährdungen diente zur Prüfung der Vollständigkeit. Es entstand eine Liste mit zurzeit 60 SPH. Die Liste der SPH wird mit der fortschreitenden Entwicklung der Ereignisbäume im Risk Control Model RCM nachgeführt und angepasst.“ [KPG08, S. 11]

Risk Control Model (RCM)

„Ausgehend von den SPH werden die Ereignisse mit Situationen und Ortsbeschreibungen (soweit zum Verständnis erforderlich), eventuellen Verzweigungen bis zu den resultierenden Unfällen in Ereignisbäumen grafisch dargestellt. Die SPH münden nur dann in Unfallereignissen, wenn weder Barrieren noch Neutralisierende Faktoren wirken. Barrieren sind

Sicherungseinrichtungen, mit denen die Gefährdung aktiv beherrscht werden kann, gegebenenfalls nur partiell. Es können mehrere Barrieren in einem Strang vorhanden sein." [KPG08, S. 11]

Erörterung der Zielsetzung

Die Zielsetzung des Projekts ROSA ist auf die Bewertung von „Sicherheitseinrichtungen" gerichtet, um diese unter Kosten-Nutzen-Aspekten optimal einzusetzen. Zentrale Ansatzpunkte sind „Starting Point Hazards". Es handelt sich dabei um eine Liste von Gefährdungen, die beim Betrieb eines „rudimentären Eisenbahnsystems" auftreten können und die mit Hilfe von hinzuzufügenden Sicherheitseinrichtungen beherrscht werden müssen. Die Starting Point Hazards sollen auf Basis des „rudimentären Eisenbahnsystems ohne Sicherheitseinrichtungen", auch als „Basic System" bezeichnet, abgeleitet worden sein; eine Liste dafür definierter Basisfunktionen („Basic generic safety functions") oder eine andere Form der Systemdefinition ist in [KPG08], im Gegensatz zu den drei Listen „Starting Point Hazards", „Barrieren" und „Neutralisierende Faktoren", nicht enthalten. Diese Gewichtung steht im Kontext zur Zielsetzung und legt zugleich die Vermutung nahe, dass mit ROSA nicht das Ziel verfolgt worden ist, eine umfassende generische Referenz für Betriebsverfahren zu schaffen.

Um die vorstehende Vermutung zu verifizieren und weil dem Autor dieser Arbeit keine weitergehenden Veröffentlichungen zu dem Projekt ROSA bekannt geworden sind, sind die aus dem „Basic System" abgeleiteten „Starting Point Hazards" untersucht worden, inwieweit sie Merkmale enthalten, die auf eine systematische Ableitung der Gefährdungen auf Basis einer funktionalen Betrachtung schließen lassen. Als Ergebnis dieser Untersuchung (Anhang 1) ist festzuhalten, dass die SPH im Wesentlichen situativ, ursachen- und folgenbezogen formuliert worden sind. Bei den situativ geprägten SPH kann zudem zwischen Situationen, die im System Eisenbahn üblich sind und betrieblich beherrscht werden müssen, sowie Situationen unterschieden werden, die sich erst nach dem Eintreten eines gefährlichen Funktionsversagens ergeben können. Die festgestellten Unterschiede in der Art der Formulierungen erlauben den Rückschluss, dass die SPH nicht auf Basis einer einheitlich funktional aufgebauten Systemdefinition abgeleitet worden sind. Eine Überschneidung des Projekts ROSA mit der vorliegenden Arbeit bezüglich der Definition einer generischen Referenz für Betriebsverfahren darf damit als ausgeschlossen angenommen werden.

Erörterung der Methodik

Im Hinblick auf die Verwendung der Sanduhrsymbolik sowohl im Projekt ROSA als auch in der vorliegenden Arbeit wird an dieser Stelle auf die Unterschiede verwiesen. Die im ROSA-Modell genutzte Symbolik (Bild 16) scheint auf den ersten Blick bis auf die Drehung um 90° prinzipiell jener der CENELEC-Sanduhr zu gleichen, in der das Ereignisbaum-Dreieck „oben" angeordnet ist. Dieses Dreieck unterscheidet sich jedoch in einem wesentlichen inhaltlichen und methodischen Punkt von der CENELEC-Sanduhr als auch von der in dieser Arbeit modifizierten Sanduhr: Barrieren sind gemäß ROSA-Modell *„Sicherungseinrichtun-*

gen, mit denen die Gefährdung aktiv beherrscht werden kann". Die Anordnung dieser Barrieren im Ereignisbaum, d.h. hinter der Gefährdung bedeutet, dass die „aktive Beherrschung" der Gefährdung im ROSA-Modell erst nach dem Gefährdungseintritt beginnt. Damit unterscheidet sich das ROSA-Modell in sehr grundlegender Weise von der Modellvorstellung der CENELEC-Normen, nach der die Beherrschung einer Gefährdung darin besteht, eine Funktion so durch technische oder prozedurale Systeme zu realisieren, dass das Eintreten der zugehörigen Gefährdung möglichst verhindert wird, d.h. die Gefährdung nicht über ein zulässiges Maß hinaus auftreten kann. [15]

Es ist festzustellen, dass der Ereignisbaum des ROSA-Modells als Barrieren bezeichnete Funktionsrealisierungen enthält, die eigentlich nicht den Übergang von einer eingetretenen Gefährdung zu einem Unfall, sondern aufgrund ihrer Art der Realisierung bereits das Eintreten der Gefährdung verhindern sollen. Das bedeutet, dass im ROSA-Modell alle im Basic System rudimentär realisierten „Basic generic safety functions" im Ereignisbaum eine funktionale Entsprechung als „Advanced generic safety functions" besitzen werden. Sie sind funktional deckungsgleich und ließen sich durch dieselben betrieblichen Funktionen ausdrücken und würden damit dieselben betrieblichen Gefährdungen besitzen. Aus diesem Grunde ist auch die Unterscheidung zwischen „basic" und „advanced" sowohl aus funktionaler Sicht als auch vom generischen Anspruch her nicht möglich und könnte nur auf die Art der Realisierung bezogen angebracht sein, um z. B. deren Wertigkeit, z. B. in Bezug auf die Erfüllung von Sicherheitsanforderungen, zu unterscheiden.

Nur jene im ROSA-Ereignisbaum als Barrieren aufgeführten „Advanced generic safety functions", die funktional keiner der „Basic generic safety functions" entsprechen und somit nicht als betriebliche Funktion ausgedrückt werden können, sind tatsächlich zusätzliche Funktionen. Im Rahmen dieser Arbeit werden entsprechende Funktionen als „planmäßige Barrieren" definiert (s. a. Bild 10), in dem Application Guide zur EN 50126 als „Containment" [CLC/TR 50126-2]; sie werden eingesetzt, um die Entwicklung von der eingetretenen Gefährdung zum Unfall zu beeinflussen. Die „Neutralisierung factors" entsprechen den zufälligen Barrieren und beeinflussen ebenfalls die Entwicklung zu einem Unfall.

[15] Der Begriff „Eine Gefährdung beherrschen" wird im Rahmen von Sicherheitsbetrachtungen häufig verwendet. Sein Wortlaut kann theoretisch in zweierlei Hinsicht interpretiert werden: A) Eine aufgrund des Versagens einer betrachteten Funktion bereits eingetretene Gefährdung wird „beherrscht", indem der Unfalleintritt durch eine geeignete andere Funktion nach Möglichkeit verhindert wird. B) Eine von einer Funktion potentiell ausgehende Gefährdung wird durch die Realisierung der betrachteten Funktion „beherrscht", indem das Eintreten der Gefährdung nach Möglichkeit verhindert wird. In den Sicherheitsbetrachtungen wird allgemein Interpretation B) verstanden. Die Gefährdungsbeherrschung wird deshalb nach den einschlägigen Normen im unteren Dreieck der Sanduhr betrachtet; Maßnahmen, die im Sinne von A) verstanden werden, werden also dem oberen Dreieck zugeordnet und nicht als „Beherrschung" bezeichnet, sondern im Sinne des im Application Guide zur EN 50126 angegebenen englischen Begriffs „Containment" (vgl. a. Bild 12) als Abwehr, Einkapselung oder Begrenzung oder auch, wie in dieser Arbeit, als „planmäßige Barrieren".

Der Unterschied in den Vorgehensweisen wird im Bild 17 anhand des in ROSA identifizierten SPH *„Train detection failed“* dargestellt. Dazu werden dem SPH entsprechenden Barrieren und neutralisierenden Faktoren der ROSA-Sanduhr zugeordnet und zugleich Verweise auf die Bereiche der modifizierten Sanduhr eingetragen, denen sie dort zugeordnet würden.

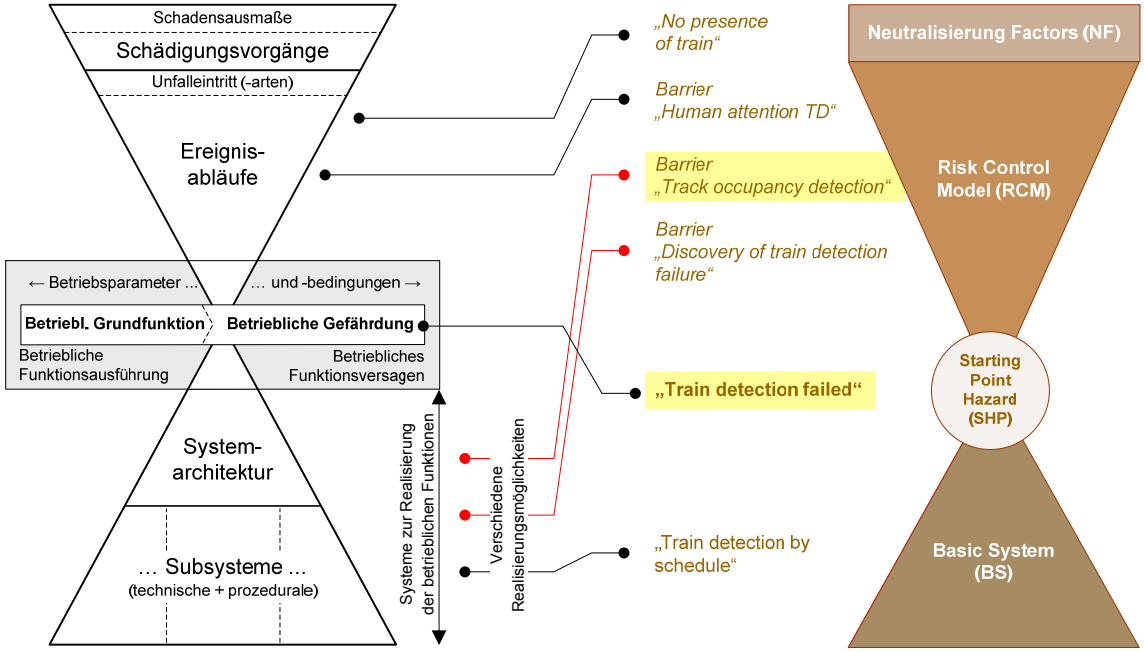


Bild 17: Vergleich der ROSA-Sanduhr mit der modifizierten Sanduhr

Schlussfolgerung

Dem ROSA-Modell liegt mit hoher Wahrscheinlichkeit keine funktional definierte Systembeschreibung zugrunde. Insbesondere darf davon ausgegangen werden, dass keine betrieblichen Funktionen im Sinne des Ziels der vorliegenden Arbeit definiert worden sind. In dem Modell wird ferner die „Sanduhr“ in einer auch von den Normen EN 50126 und EN 50129 abweichenden Form interpretiert. Insbesondere wird die Wirkungskette verletzt, da zwischen der Gefährdung und dem Unfall *„Barrieren“* angeordnet werden, die dort formal der Beherrschung der Gefährdung dienen sollen, letztlich aber eine Realisierung der Funktion sind. Auf diese Weise werden die Ursachen der Gefährdung nicht vor dem Eintritt der Gefährdung, sondern erst zwischen ihr und dem Unfall eingeordnet. Der Grund der Verletzung der Wirkungskette dürfte ebenfalls in dem Nichterkennen der funktionalen Gemeinsamkeiten zwischen den *„Basic generic safety functions“* und Teilen der *„Advanced generic safety functions“* liegen.

3.2.3 Fahrzeugfunktionen gemäß prEN 15380-4

Für das Teilsystem Fahrzeug liegt mit der Vornorm prEN 15380-4 eine mit generischem Anspruch angelegte Funktionsliste vor. Sie basiert auf dem Entwurf der DIN 25002 Teil 5 sowie auf der vom europäischen Verband der Bahnindustrie (UNIFE) entwickelten MODTrain Struktur und befindet sich noch in der Entwicklung [BEP08].

Obwohl das Teilsystem Fahrzeug nicht Gegenstand der vorliegenden Arbeit ist, ist die prEN 15380-4 aus mehreren Gründen auch für die Entwicklung der angestrebten generischen Funktions- und Gefährdungsliste für Betriebsverfahren von Interesse:

- Betriebsverfahren sind das zentrale Element, über das das mobile Teilsystem Fahrzeug in den Betrieb des Gesamtsystems Eisenbahn eingebunden wird. Die prEN 15380-4 enthält mit der Hauptfunktion *„Integrate the vehicle into the complete railway system“* eine unmittelbare fahrzeugseitige Entsprechung.
- Als Teile des komplexen Systems Eisenbahn besitzen Fahrzeuge und Betriebsverfahren unabhängig von ihrer Realisierung logische und physikalische Schnittstellen[16]. Diese müssen in den Systemdefinitionen und Listen vorhanden und in geeigneter Weise aufeinander abgestimmt sein.
- Auch mit dem Status einer Vornorm besitzt die Liste bereits eine Anerkennung in der Fachwelt, die bei der Entwicklung einer Funktionsliste für Betriebsverfahren zu berücksichtigen ist. Auch wenn nicht damit zu rechnen ist, dass sie in ihren Grundzügen nennenswert verändert werden wird, sind Verbesserungen oder Ergänzungen nicht ausgeschlossen, da z.B. ihre Funktionsstruktur schwer auf Sicherungssysteme übertragbar ist [WK07]. Aus der Definition der generischen Funktionen für das Teilsystem Betriebsverfahren könnten sich folglich Hinweise zu Verbesserungen oder zu Anpassungen sowie zur Definition bzw. Präzisierung von Schnittstellen ergeben.
- Ferner ist zu prüfen, ob die Fahrzeugliste Anhaltspunkte, Anregungen und zu berücksichtigende Vorgaben enthält.

[16] Die physikalischen Schnittstellen befinden sich an der mechanischen Außenhaut des Fahrzeugs einschließlich seiner Räder. Die logischen Schnittstellen sind i.d.R. nicht an der Außenhaut des Fahrzeugs zu finden, sondern i.d.R. auf dem Fahrzeug. Sie grenzen unter logischen Gesichtspunkten z.B. das Fahrzeug von den Betriebsverfahren ab, deren Funktionen u.a. in Form des Triebfahrzeugführers auf dem Fahrzeug realisiert werden können.

Relevanz der prEN 15380-4 für Betriebsverfahren

In der prEN 15380-4 werden auf der obersten Ebene neun Hauptfunktionen[17] definiert, die auf bis zu drei darunter liegenden Ebenen heruntergebrochen werden. Nicht alle diese Funktionen besitzen eine derart hohe Schnittstellenrelevanz zu Betriebsverfahren, dass sie im Rahmen der in diesem Kapitel vorgenommenen Untersuchung der Ausgangssituation detailliert betrachtet werden müssten. Aber für die für den Bereich der Betriebsverfahren als besonders relevant anzusehenden Hauptfunktionen muss untersucht werden, in welcher Weise deren in der zweiten und dritten Ebene definierten Teilfunktionen beschrieben werden und welche Verbindungen zu Betriebsverfahren bestehen. Das Ziel der Analyse ist eine Aussage, über eine mögliche Verwendung und Einbindung der Funktionsliste der prEN 15380-4 bei der Erstellung der generischen Funktions- und Gefährdungsliste für Betriebsverfahren.

Um die für Betriebsverfahren wesentlichen Hauptfunktionen zu identifizieren, wird in der Tabelle 4 die funktionale Relevanz der neun Hauptfunktionen als „gering", „mittel" und „hoch" eingestuft. Dazu wird abgeschätzt, ob es für die Hauptfunktionen des Fahrzeugs eine unmittelbare Entsprechung in den Betriebsverfahren gibt oder ob die Funktionen überwiegend fahrzeuginternen Charakter besitzen, d.h. der Erfüllung originärer Fahrzeugaufgaben dienen. Für die Einstufung ist dagegen unerheblich, ob ein Versagen der Funktion im Betrieb zu einem Unfall führen kann, da bei allen Funktionen davon auszugehen ist, dass sich das Versagen nahezu jeder Funktion erst während des Betriebs als Unfall auswirken wird. Von einer Einstufung in „nicht relevant" wird Abstand genommen, da in einem komplexen System wie der Eisenbahn eine Relevanz kaum ausgeschlossen werden kann.

Tabelle 4: Relevanz der Hauptfunktionen der prEN 15380-4 für Betriebsverfahren

Hauptfunktionen [prEN 15380-4]		**Funktionale Relevanz für Betriebsverfahren**	
		Erläuterung	**Einstufung**
B	*Carry and protect passenger, train crew and load*	Die B-Funktionen sind vom Fahrzeug zu erbringen, sie werden nicht durch Betriebsverfahren realisiert. Ihre Ausführung muss allerdings während des Betriebs sicher gewährleistet werden.	gering
C	*Provide appropriate conditions to passenger, train crew and payload*	Die C-Funktionen sind vom Fahrzeug zu erbringen, sie werden nicht durch Betriebsverfahren realisiert. Ihre Ausführung muss allerdings während des Betriebs sicher gewährleistet werden.	gering

[17] Die Hauptfunktionen werden in der prEN 15380-4 mit den Codebuchstaben B, C, D, E, F, G, H, J, K gekennzeichnet. Der Code ihrer Teilfunktionen beginnt ebenfalls mit diesen Buchstaben. Der sprachlichen Handhabbarkeit wegen wird nachfolgend die Bezeichnung *B-(Teil-)Funktionen* usw. genutzt.

Hauptfunktionen [prEN 15380-4]		**Funktionale Relevanz für Betriebsverfahren**	
		Erläuterung	**Einstufung**
D	*Provide access and loading*	Die D-Funktionen gehören zu Prozessen, die vor der Durchführung von Fahrten ablaufen. Sie sind so durchzuführen, dass das Ergebnis ihrer Abwicklung während des Betriebs aufrecht erhalten wird.	gering
E	*Connect vehicles and/or consists*	Das Verbinden der Fahrzeuge zu betriebsbereiten Zügen ist eine vorbereitende Aufgabe, die fahrzeugseitig zu erbringen ist. Im Fahrbetrieb der Züge ist die Relevanz der E-Funktionen als gering anzusehen. Eine höhere Relevanz ergibt sich bei Fahrzeugbewegungen, die dem Zusammenstellen von Zügen dienen. Auch bei Betriebsvorgängen, in denen an sich fahrbereite Züge gekuppelt werden (Train Coupling and Sharing), ist eine höhere Relevanz zu Betriebsverfahren zu sehen.	gering /mittel
F	*Provide energy*	Die Versorgung mit Energie und Betriebsstoffen umfasst Prozesse, die dem Fahrzeug, der erforderlichen Infrastruktur und der Fahrtvorbereitung zuzurechnen sind. Da bei elektrischer Traktion die Energie unmittelbar während des Betriebs zugeführt wird, ergibt sich in diesen Fällen ein als unmittelbar einzustufender Bezug.	gering; nur bei E-Traktion höher
G	*Accelerate, maintain speed, brake and stop*	Die G-Funktionen dienen der fahrzeugseitigen Umsetzung von Fahrzeugbewegungen. Über das Geben der Fahrterlaubnis haben sie einen direkten Bezug zu Betriebsverfahren.	**hoch**
H	*Provide train communication, monitoring and control*	Der Begriff „Fahrzeug übergeordnet leiten“ bedeutet nicht das Leiten i.S. einer netzweiten Betriebsführung, sondern bezieht sich auf die innerhalb des Fahrzeugs zu leitenden, zu überwachenden und zu kontrollierenden Prozesse einschließlich der erforderlichen Kommunikation.	mittel
J	*Support and guide the train on the track*	Fahrzeugseitig bereitzustellende Einrichtungen, die die Spurführung gewährleisten.	Gering
K	*Integrate the vehicle into the complete railway system*	Die K-Funktionen sind im Prinzip eine funktionale Generalklausel zur Einbindung des Fahrzeugs in das Gesamtsystem. Bezüglich des bewegten oder unmittelbar zu bewegenden Fahrzeugs ist diese Einbindung eine unmittelbare Aufgabe der Betriebsverfahren.	**hoch**

Ergänzung der Liste in [BEP08, S. 51, 205]			
L	*Zusätzliche Funktionen für den Bereich der Leit- und Sicherungstechnik*	Die L-Funktionen sind in [BEP08] als schnittstellenartige Ergänzung der K-Funktionen definiert worden. Sie besitzen damit automatisch eine hohe funktionale Relevanz für den Bereich der Betriebsverfahren.	**hoch**

Insbesondere für die G-Hauptfunktionen *„Accelerate, maintain speed, brake and stop“*, die K-Hauptfunktion *„Integrate the vehicle into the complete railway system“* sowie die ergänzend definierten L-Hauptfunktion sind enge Bezüge zu Betriebsverfahren zu erwarten. Sie werden im Folgenden insbesondere auf mögliche Überschneidungen mit Funktionen untersucht, die im Bereich von Betriebsverfahren liegen könnten.

G-Hauptfunktion „Accelerate, maintain speed, brake and stop”

Mit der G-Hauptfunktion werden der Formulierung nach alle für einen betrieblichen Fahrzyklus wesentlichen Zustände der Fahrbewegung angesprochen: Beschleunigen, Geschwindigkeit halten, Abbremsen und Halten incl. Stillstandssicherung (Bild 18).

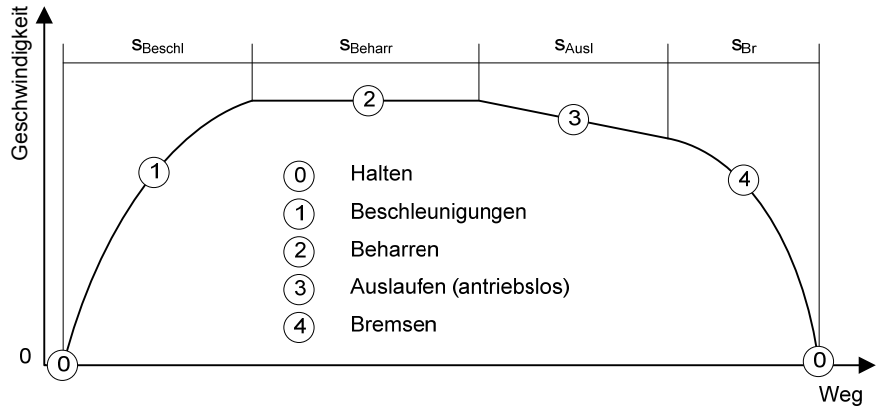


Bild 18: Betrieblicher Fahrzyklus

Aus betrieblicher Sicht ist somit auf der Hauptfunktionsebene ein unmittelbarer Bezug zu Betriebsverfahren erkennbar. Allerdings kann die in dieser Weise formulierte Hauptfunktion sowohl dem Fahrzeug als auch den Betriebsverfahren zugehörig interpretiert werden: Fahrzeugseitig als Funktion zum Erzeugen und Steuern der Kräfte und betrieblich als das

Steuern der Fahrzeugbewegung entsprechend der Fahrtvorgaben im Sinne einer Geschwindigkeitseinhaltung[18].

Um die detaillierter formulierten G-Teilfunktionen einordnen zu können, wird ausgehend von den beiden vorstehenden Interpretationsmöglichkeiten eine Schnittstelle definiert. Sie liegt zwischen der betrieblichen Geschwindigkeitsregelung und der fahrzeugseitigen Regelung der Erzeugung der angeforderten Antriebs- und Bremskräfte und spiegelt den folgenden funktionalen Zusammenhang wieder: Um betrieblich die Geschwindigkeit den Fahrtvorgaben anpassen zu können, müssen fahrzeugseitig die erforderlichen Kräfte geregelt werden. Die Schnittstelle ist somit durch die betrieblich motivierte Anforderung von Antriebs- und Bremsleistungen charakterisiert. Zu beachten ist dabei jedoch, dass bei dieser Schnittstellenanordnung fahrzeugseitig, d.h. in bzw. auf dem Fahrzeug nicht nur Fahrzeugfunktionen, sondern auch Betriebsverfahrensfunktionen wie z.B. die Geschwindigkeitsregelung realisiert werden (Bild 19).

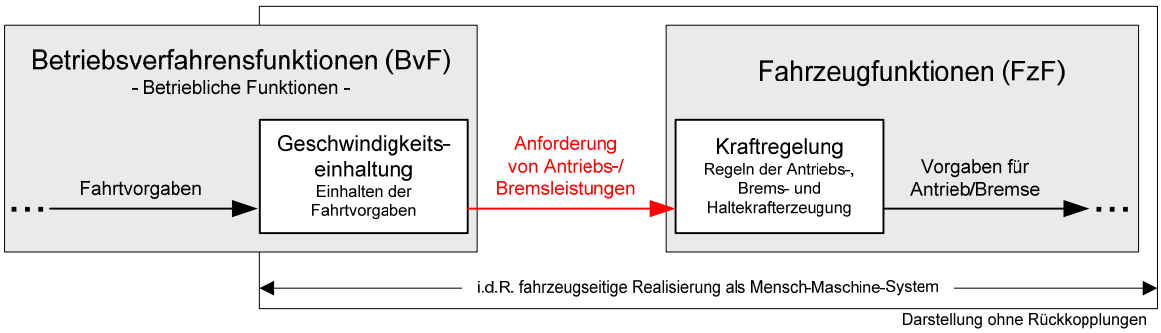


Bild 19: Definition einer vorläufigen Schnittstelle für die G-Funktionen

Da an beiden Funktionsarten i.d.R. der Triebfahrzeugführer als Träger mehrerer Funktionen beteiligt ist, wird die Unterscheidung zwischen Betriebsverfahrensfunktion und Fahrzeugfunktion nicht immer wahrgenommen[19]. Bei funktionaler Betrachtung ergibt sich eine solche Aufteilung allerdings automatisch, da das Regeln der Geschwindigkeit zur Einhaltung betrieblicher Fahrtvorgaben das Betriebsverfahren schon in logischer Hinsicht vervollständigt und gegenüber den Fahrzeugfunktionen abgrenzt. Diesem Gedanken folgen auch die

[18] Jeder Zustand der Fahrbewegung kann mit Hilfe der Geschwindigkeit ausgedrückt werden: Über den Weg als konstante Geschwindigkeit einschließlich V = 0 für das Halten sowie als wegabhängige Kurven bei Beschleunigungs- und Verzögerungsvorgängen.

[19] Wegen der Übernahme i.d.R. mehrerer Funktionen durch den Triebfahrzeugführer wird die logische Grenze zwischen betrieblichen und fahrzeugseitigen Funktionen nur schwer wahrgenommen. Deshalb ein einfaches Sinnbild: Aus der Fahrdienstvorschrift erfährt der Triebfahrzeugführer, weshalb und wann er zu bremsen hat (betriebliche Funktionen), aus der „Bedienungsanleitung“ für das Fahrzeug dagegen, wie er das Fahrzeug zu bedienen hat, damit es die Bremsleistung erbringt (Fahrzeugfunktionen).

EU-Interoperabilitätsrichtlinie und die zugehörigen technischen Spezifikationen für die Interoperabilität (TSI)[20].

Die Analyse der Teilfunktionen der G-Hauptfunktion *„Accelerate, maintain speed, brake and stop“* (Anhang 2) ergibt, dass alle G-Teilfunktionen nicht nur unter physikalischen, sondern auch unter logischen Gesichtspunkten als Fahrzeugfunktionen einzustufen sind. Mit ihnen soll sichergestellt werden, dass das Fahrzeug die betrieblich angeforderten Antriebs- und Bremsleistungen erbringt. Dies geschieht durch das unmittelbare Erzeugen der entsprechenden Kräfte und die Steuerung und Abstimmung der zur Krafterzeugung eingesetzten Einrichtungen. Die in der Tabelle 4 zunächst erfolgte Einstufung der G-Funktionen als „hoch“ hat sich nicht bestätigt. Die G-Funktionen brauchen im Rahmen dieser Arbeit nicht weiter betrachtet werden.

K-Hauptfunktion „Integrate the vehicle into the complete railway system”

Mit der K-Hauptfunktion soll die Einbindung des Fahrzeugs in das Gesamtsystem Eisenbahn erfolgen. Die Einbindung eines Fahrzeugs umfasst grundsätzlich zwei wesentliche Punkte: Zum einen die physikalische Kompatibilität zur gebauten Infrastruktur und zum anderen die Verknüpfung mit einem Betriebsverfahren. Für die K-Teilfunktionen wird analysiert, inwieweit sie unter logischen Gesichtspunkten dem Fahrzeug oder dem Betriebsverfahren zuzuordnen sind. Die Analyse (Anhang 3) zeigt, dass die K-Funktionen eindeutig der Verknüpfung des Fahrzeugs mit den Betriebsverfahren dienen sollen. Es ist deshalb festzuhalten, dass alle als K-Funktionen aufgeführten Formulierungen dem Bereich der Betriebsverfahren und den damit verbundenen betrieblichen Funktionen und nicht den Fahrzeugfunktionen zuzuordnen sind. Allerdings werden die K-Funktionen oft auf dem Fahrzeug realisiert. Der dabei unvermeidliche „Spagat“ zwischen logischer und physikalischer Schnittstelle führt bei der Definition dieser Funktionen zu Problemen in der begrifflichen Zuordnung.

Da für eine fahrzeugseitige Realisierung betrieblicher Funktionen entsprechend gestaltete Einrichtungen auf dem Fahrzeug vorgehalten werden, muss eine gewisse Vorstellung für die Systemarchitektur vorliegen. Dies führt bei der an sich generisch beabsichtigten Formulierung der betreffenden Funktionen leicht zu realisierungsnahen Formulierungen. Dies kommt dadurch zum Ausdruck, dass die formulierten K-Teilfunktionen überwiegend einen in Richtung der technischen Realisierung anfordernden als einen aus betrieblicher Sicht

[20] In der EU-Interoperabilitätsrichtlinie wird das Teilsystem Fahrzeug an *„Mensch-Maschine-Schnittstellen (Zugführer, Fahrpersonal, Fahrgäste unter Berücksichtigung der Bedürfnisse von Personen mit eingeschränkter Mobilität), […]“* abgegrenzt [2008/57/EG]. In der technischen Spezifikation für die Interoperabilität des Teilsystemsfahrzeuge (TSI Fahrzeuge) wird dementsprechend unter 2.1 *„Zugpersonal (Triebfahrzeugführer und anderes Bordpersonal)“* ausdrücklich als Bestandteil des Teilsystems Fahrzeug ausgeschlossen [2008/232/EG]. In der TSI Verkehrsbetrieb und Verkehrssteuerung wird im Abschnitt 2.1 die diesbezügliche Funktion *„des Führens von Zügen“* mit dem Wort *„insbesondere“* nachdrücklich dem Teilsystem Verkehrsbetrieb und Verkehrssteuerung zugerechnet [2006/920/EG].

funktionalen Charakter besitzen. Bei den Formulierungen handelt es sich um Anforderungen an die fahrzeugseitig zu gewährleistenden Schnittstellen für den Fall, dass die entsprechenden betrieblichen Funktionen im Sinne der K-Funktionen auf dem Fahrzeug realisiert werden sollen. Funktionsformulierungen, aus denen unmittelbar ein *betrieblicher Zweck oder ein betrieblich zu erreichendes Ziel*[21] hervorgeht, sind unter den K-Funktionen kaum zu finden.

Ergänzte L-Funktionen

BEPPERLING leitet in [BEP08] ausgehend von der Interpretation der K-Funktionen als an der physikalischen Schnittstelle liegende Fahrzeugfunktionen zwischen dem Fahrzeug und der Strecke weitere Funktionen ab. Die *„Grundidee“* dieser *„generischen Systemdefinition“* bestehe darin, *„dass ausgehend von einer vollständigen Beschreibung der Fahrzeugfunktionen und zusätzlich einer vollständigen Schnittstellenbeschreibung alle Funktionen und somit auch Gefährdungen für das Eisenbahnsystem auf der für BP-Risk korrekten Ebene ermittelt werden können“*. Dazu wird von ihr die in Bild 20 wiedergegebene Schnittstellendefinition zugrunde gelegt.

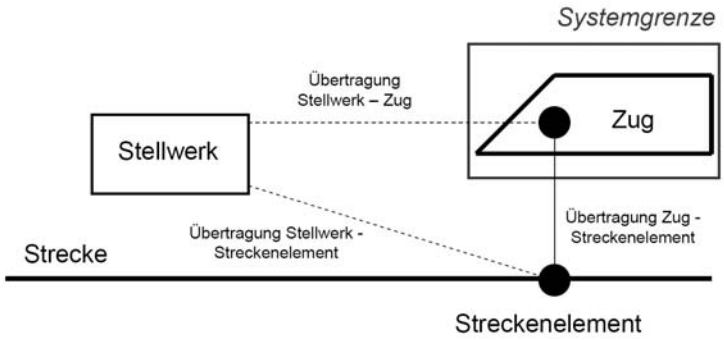


Bild 20: Schnittstellendefinition in [BEP08, S. 50]

Mit dem Codebuchstaben L werden in [BEP08] *„alle Streckenfunktionen“* gekennzeichnet, *„die an den Fahrzeugschnittstellen beschrieben wurden“*. Die ebenfalls in Bild 20 dargestellte Schnittstelle *Stellwerk-Zug wurde „erst einmal nicht betrachtet, da es sich dort in der Regel um eine zentrale Ansteuerung per Funk, z. B. ausgehend von einer Streckenzentrale, (Radio Block Center, RBC) handelt“*. Bei einem solchermaßen definierten System zur Durchführung des Betriebs scheint bereits die Vorstellung einer Systemarchitektur einschließlich einer Funktionsverteilung zwischen Zug, Strecke und Stellwerk vorzuliegen. Im Anhang 4 wird deshalb auch geprüft, inwieweit die definierten Teilfunktionen bezogen auf Betriebsverfahren noch als generisch angesehen werden können.

[21] Nach IEC 61226 (deutsche Übersetzung [BEP08, s. 46]) wird eine Funktion als „bestimmter Zweck oder zu erreichendes Ziel“ definiert, „das spezifiziert oder näher beschrieben werden kann, ohne Bezug auf die physikalischen Mittel zu nehmen“. Legt man diesen Maßstab für betriebliche Funktionen zugrunde, müssten sie so formuliert sein, dass der betriebliche Zweck oder das betrieblich zu erreichende Ziel erkennbar wird.

Die Analyse der prEN 15380-4 und die Analyse der in [BEP08] ergänzten L-Funktionen führt zu folgenden Ergebnissen:

- Die in der prEN 15380-4 unter CODE K sowie die in [BEP08] unter CODE L aufgeführten Funktionen betreffen einen Bereich des Systems Eisenbahn, der unter logischen Gesichtspunkten nicht den klassischen Fahrzeug- oder Streckenfunktionen, sondern eindeutig den Betriebsverfahren zuzuordnen ist. Die Funktionen sind für die Abwicklung der originären Aufgaben eines Fahrzeugs nicht erforderlich. Sie dienen allein der Durchführung des Eisenbahnbetriebs und seiner Sicherung.
- Der Bezug der K-Funktionen zum Fahrzeug ergibt sich lediglich aus der Möglichkeit, sie ganz oder in Teilen fahrzeugseitig, d.h. auf dem Fahrzeug realisieren zu können. Wenn dies als Lösung beabsichtigt wird, muss das Fahrzeug in Abhängigkeit von der Funktionsrealisierung entsprechende technische und funktionale Anforderungen erfüllen.
- Aus vorstehenden Gründen ist aus dem Blickwinkel der Betriebsverfahren der im Bild 21 dargestellten Zuordnung der *„K-Funktionen“* zu *„Fahrzeugfunktionen“* und der *„L-Funktionen“* zu *„Streckenfunktionen“* zu widersprechen. Beide Funktionsgruppen zusammen bilden aus betrieblicher Sicht eine funktionale Einheit. Es sollte daher, wenn differenziert werden soll, von betrieblichen Teilfunktionen mit fahrzeug- oder streckenseitigen Realisierungen gesprochen werden.

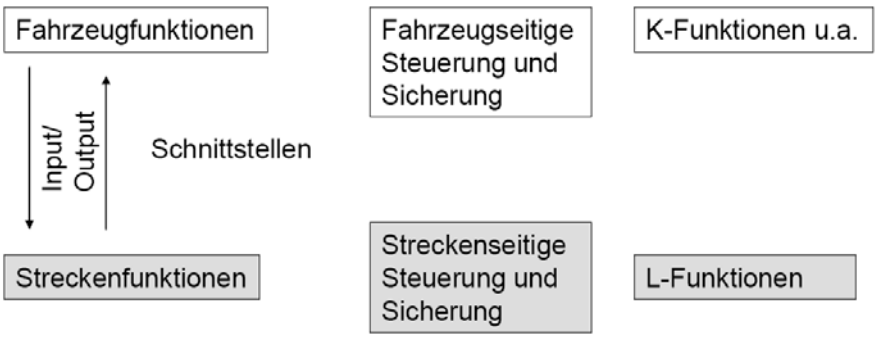


Bild 21: Schnittstellenbeschreibung aus [BEP08, S. 51]

- Nicht alle in der Liste der K- als auch in jener der L-Funktionen aufgeführten Formulierungen sind als betriebliche Grundfunktionen anzusehen, die über einen betrieblichen Zweck oder ein betriebliches Ziel definiert worden sind. Ein großer Teil von ihnen ist im Stil von Anforderungen formuliert und enthält bereits Vorstellungen für bestimmte Systemarchitekturen, deren Subsysteme die nicht näher spezifizierten betrieblichen Grundfunktionen realisieren sollen. Im Bild 22 wird eine grobe Zuordnung der K- und L-Funktionen zur modifizierten Sanduhr vorgenommen. Bei dem Versuch, die Funktionen exakter zuzuordnen, zeichnet sich ab, dass sich unterhalb der Ebene der Betrieblichen Grundfunktionen eine bis zu den Subsystemen reichende hierarchische Funktionsstruktur einstellen wird, innerhalb derer die Grenze zwischen generisch definierbaren und realisierungsabhängigen Funktionen liegen wird.

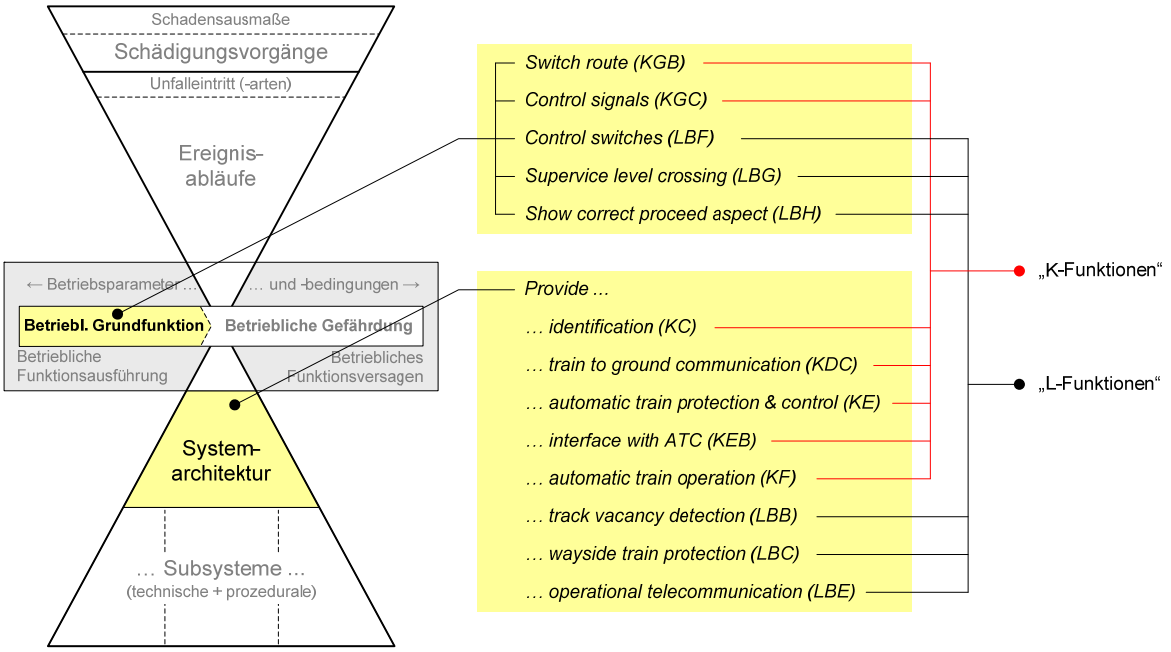


Bild 22: Einordnung von K- und L-Funktionen in die modifizierte Sanduhr

- Das Beschreiben technischer oder funktionaler Anforderungen gibt allein noch nicht den betrieblichen Zweck oder das betrieblich zu erreichende Ziel der betrieblichen Funktion wieder. Mehrere der für die *„K-“* und *„L-Funktionen“* gewählten Formulierungen verstoßen deshalb unter betrieblichen Gesichtspunkten gegen Grundsätze, die in der IEC 61226 für die Definition von Funktionen genannt werden.
- Nicht alle *„K-“* und *„L-Funktionen“* können im betrieblichen Sinne als generisch angesehen werden, da sie bereits bestimmten Realisierungsvorstellungen unterliegen. Es ist jedoch auf der generischen Betrachtungsebene unerheblich, ob z.B. das Abbremsen eines Fahrzeugs von einem Triebfahrzeugführer, der einen restriktiven Fahrtbegriff von einem ortsfesten Signal aufgenommen hat, oder von einem automatischen System, dem per Funk entsprechende Daten übermittelt werden, eingeleitet wird. Funktional entscheidend, und allen Realisierungen gemeinsam, ist das *Geben und Empfangen des Fahrtbegriffs* sowie das *Einleiten der Bremsung*[22].
- Es ist festzustellen, dass zwischen dem fahrzeugseitig-funktionalen und dem betrieblich-funktionalen Betrachtungsraum eine Diskrepanz besteht: Denn fahrzeugseitig sind nur jene betrieblichen Funktionen von Interesse, aus denen sich Schnittstellen ergeben, die im Rahmen der technischen Fahrzeugrealisierung zu berücksichtigen sind. Ebenfalls das Fahrzeug betreffende betriebliche Aspekte, wie z.B. die Behandlung von

[22] Diese generische Beschreibung träfe ebenso auf Systeme mit Führerstandsignalisierungen zu. Gleiches gilt für Systeme mit fahrwegseitigem Antrieb und Bremse, wie z.B. einer fahrerlosen Transraipd-Variante. Im letzteren Fall entfiele sogar die fahrzeugseitige Realisierung, sie wäre in diesem Fall streckenseitig.

Lademaßschreitungen, würden bei einer ausschließlichen Abstützung auf die Fahrzeugliste fehlen. Auch der Ausschluss zeitgleicher Fahrwegbeanspruchungen, eine der Kernaufgaben der Betriebsverfahren, ergibt sich nicht aus der Schnittstellenbetrachtung und die abgeleitete Funktion *LBB track vacancy detection* trägt im Sinne einer Teilfunktion nur dazu bei.

Schlussfolgerungen

Die in der prEN 15380-4 enthaltenen K-Funktionen und die ergänzten L-Funktionen sind unabhängig von dem Ort ihrer Realisierung betrieblicher Natur und sind den Betriebsverfahren zuzurechnen. Sie decken jedoch nur einen Teil des Funktionsraums von Betriebsverfahren ab. Ferner deuten sich Unterschiede zwischen den Funktionsstrukturen von Fahrzeugen und Betriebsverfahren an; auch WEBER und KURZ berichten in [WK07] von Schwierigkeiten die Funktionsstruktur der Fahrzeugliste auf Sicherungssysteme zu übertragen. Das Ableiten von Betriebsverfahrensfunktionen aus der prEN 15380-4 wird, da die Betriebsverfahren umfassender als die ihnen enthaltenden Sicherungssysteme sind, mit mindestens denselben Schwierigkeiten verbunden sein.

Aus vorstehenden Gründen ist, um für den Bereich der Betriebsverfahren eine weitgehend umfassende generische Referenz erarbeiten zu können, die alleinige Betrachtung der Fahrzeugfunktionsliste und ihrer Ergänzung nicht ausreichend. Vielmehr muss der Betrachtungsraum darüber hinaus ausgedehnt werden. Ein entsprechender Ansatz sollte nicht dazu dienen, die bestehenden Lücken zu schließen, sondern umfassend genug sein, eine Kontrolle und ggf. neue Einordnung insbesondere der K- und L-Funktionen aus Sicht der Betriebsverfahren zu ermöglichen. Die Einbeziehung von mit dem Anwendungsgebiet Betriebsverfahren vertrauten Experten wird analog zur Einbeziehung einschlägig vertrauter Fachleute beim Zustandekommen der prEN 15380-4 als notwendig erachtet.

Für das Formulieren der Funktionsdefinitionen für Betriebsverfahren müssen Wege gefunden werden, die betriebliche Funktionen eindeutig als solche erkennen lassen und im Sinne der IEC 61226 das Ziel bzw. den Zweck deutlicher spezifizieren..

3.2.4 EU-Interoperabilitätsrichtlinien und technische Spezifikationen (TSI)

In der EU-Richtlinie für die Interoperabilität des Eisenbahnsystems wird in deren Anhang II das Eisenbahnsystem in mehrere Teilsysteme gegliedert [2008/57/EG][23]. Diese Teilsysteme können weitgehend in die im Abschnitt 2.2 definierte Dreieckdarstellung eingeordnet werden

[23] Die Interoperabilitätsrichtlinie [2008/57/EG] ist 2008 neu gefasst worden. In ihr werden die bisher für das konventionelle transeuropäische Eisenbahnsystem und das transeuropäische Hochgeschwindigkeitseisenbahnsystem getrennten Richtlinien [96/48/EG] und [2001/16/EG] zusammengefasst. Alle drei Richtlinien beschreiben jeweils im Anhang II die im Bild 23 als 2.1. bis 2.7. aufgeführten Teilsysteme.

(Bild 23). Für den Bereich Betriebsverfahren sind dies die drei Teilsysteme *Zugsteuerung, Zugsicherung und Signalgebung* und *Verkehrsbertrieb und Verkehrssicherung* sowie in einem übergeordneten Sinne das Teilsystem *Telematikanwendungen*.

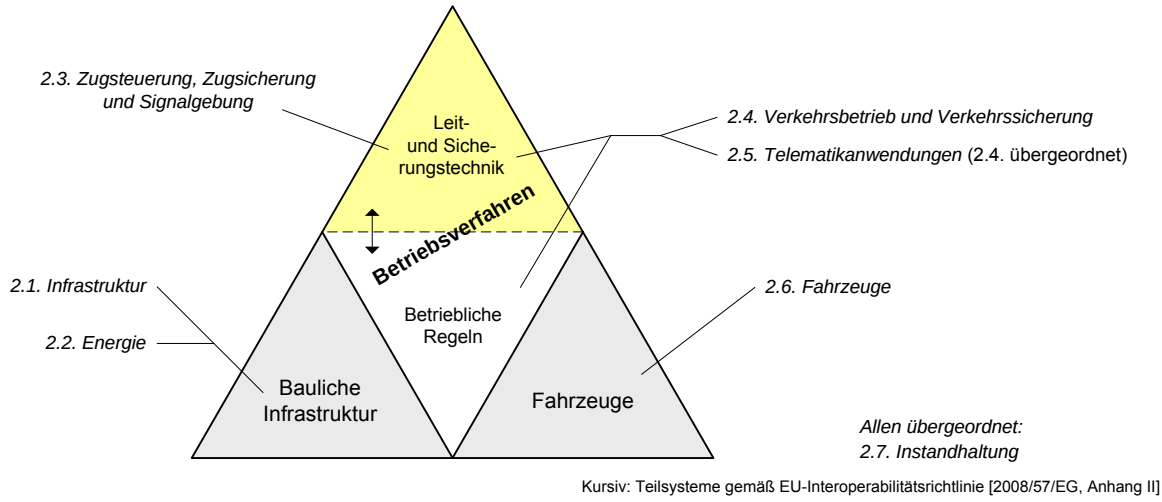


Bild 23: Funktionale Einordnung der in der Interoperabilitätsrichtlinie definierten Teilsysteme

Mit der Aussage der Richtlinie, das Eisenbahnsystem sei *„für die Zwecke der Richtlinie“* in mehrere Teilsysteme gegliedert worden, wird unterstrichen, dass mit der Richtlinie nicht der Anspruch erhoben wird, dass System Eisenbahn vollständig abzubilden. Insofern bedeutet die im Bild 23 vorgenommene Zuordnung der drei betriebsverfahrensaffinen Teilsysteme nicht, dass die Betriebsverfahren in der Richtlinie vollständig abgebildet werden. Dies wird nachfolgend beleuchtet. Die drei betriebsverfahrensaffinen Teilsysteme sollen laut [2008/57/EG] die in der Tabelle 5 wiedergegebenen Aspekte umfassen.

Tabelle 5: Teilsysteme gemäß Interoperabilitätsrichtlinie

Teilsystem und Beschreibung gemäß [2008/57/EG]	
2.3. Zugsteuerung, Zugsicherung und Signalgebung	*Alle erforderlichen Ausrüstungen zur Gewährleistung der Sicherung, Steuerung und Kontrolle der Bewegung von Zügen, die zum Verkehr im Netz zugelassen sind.*
2.4. Verkehrsbetrieb und Verkehrssteuerung	*Verfahren und zugehörige Ausrüstungen, die eine kohärente Ausnützung der verschiedenen strukturellen Teilsysteme erlauben, und zwar sowohl im Normalbetrieb als auch bei Betriebsstörungen, einschließlich insbesondere der Zugbildung und Zugführung, der Planung und der Abwicklung des Verkehrsbetriebs.* *Die Gesamtheit der erforderlichen beruflichen Qualifikationen für die Durchführung von grenzüberschreitenden Verkehrsdiensten.*

Teilsystem und Beschreibung gemäß [2008/57/EG]	
2.5. Telematik-anwendungen	*Dieses Teilsystem umfasst im Einklang mit Anhang I zwei Teile:* *a) die Anwendungen im Personenverkehr, einschließlich der Systeme zur Information der Fahrgäste vor und während der Fahrt, Buchungssysteme, Zahlungssysteme, Reisegepäckabfertigung,* *b) die Anwendungen im Güterverkehr, einschließlich der Informationssysteme (Verfolgung der Güter und der Züge in Echtzeit), Rangier- und Zugbildungssysteme, Buchungssysteme, Zahlungs- und Fakturierungssysteme, Anschlüsse zu anderen Verkehrsträgern, Erstellung elektronischer Begleitdokumente.*

Da die Zugbildung, die Zugführung, die Planung und Abwicklung des Verkehrsbetriebs ausdrücklich als Bestandteile des Teilsystems 2.4. Verkehrsbetrieb und Verkehrsteuerung erwähnt werden, ist das Teilsystem 2.5. Telematikanwendungen nicht zwingend als ein Kern der Betriebsverfahren anzusehen, sondern kann als eine Art übergeordnetes System betrachtet werden. Seine Funktionalitäten sind logistischer Natur. In diesem Sinne soll es die Schnittstellen zwischen der Betriebsdurchführung und den bei den Verkehrskunden ablaufenden Prozessen bedienen. Für das Teilsystem Telematikanwendungen gibt es bislang nur für den Bereich des Güterverkehrs eine TSI. Dem Charakter des Teilsystems entsprechend wird im Abschnitt (6) der Begründung *„die effiziente Verknüpfung der Informations- und Kommunikationssysteme der verschiedenen Fahrwegbetreiber und Eisenbahnunternehmen für wichtig erachtet“* [2006/62/EG]. Im Rahmen der vorliegenden Arbeit, in der Grundlagen für eine generische Referenz für Betriebsverfahren geschaffenen werden sollen, ist eine weitere Betrachtung des Teilsystems 2.5. Telematikanwendungen nicht notwendig.

Die Sicherung, Steuerung und Kontrolle der sich in einem Verkehrsnetz bewegenden Fahrzeuge ist als eine originäre Aufgabe von Betriebsverfahren anzusehen. Das Teilsystem 2.3. deckt somit einen unmittelbaren Teilbereich der Betriebsverfahren ab. Gleiches gilt für das Teilsystem 2.4. Verkehrsbetrieb und Verkehrssteuerung. In den TSI sind sowohl für den konventionellen Eisenbahnbahnverkehr als auch für den Hochgeschwindigkeitsverkehr nur die funktionalen und technischen Spezifikationen enthalten, die für ein freies Verkehren von Zügen notwendig sind. Es handelt sich dabei um jene Funktionalitäten, die mit Interaktionen zwischen Fahrzeug und Strecke einhergehen und deren Realisierungen deshalb fahrzeug- und streckenseitig zueinander kompatibel sein müssen. Die an sich funktional strukturierten TSI sind dementsprechend auch durch z.T. detaillierte ETCS/ERTMS-Spezifikationen geprägt. Funktionalitäten von Betriebsverfahren, die keine unmittelbaren Fahrzeug-Strecke-Interaktionen erfordern, sind in den TSI nicht enthalten. So werden z.B. das Einstellen und das Sichern von Fahrstraßen nicht in den TSI behandelt.

3.3 Analyse spezifischer Projektlisten

Im Rahmen verschiedener Risiko- und Sicherheitsanalysen, die entsprechend der CENELEC-Normen durchgeführt worden sind, sind Systemdefinitionen erstellt und Gefährdungen identifiziert und gelistet worden. Im Allgemeinen sind detaillierte Unterlagen von Risikoanalysen nicht frei verfügbar. Für die Risikoanalysen FunkFahrBetrieb (RA FFB) und Elektronisches Stellwerk (RA ESTW) liegen jedoch Fachveröffentlichungen vor. Beide Risikoanalysen decken einen großen Bereich der Betriebsverfahren ab. Dies erlaubt eine Analyse der Vorgehensweise und lässt gute Rückschlussmöglichkeiten bzgl. Der Übernahme oder Ableitung betrieblicher Funktionen erwarten. Ein besonderes Augenmerk gilt der Frage, inwieweit die Systemdefinitionen bereits funktionale Elemente enthalten und welchen Einfluss eine Systemdefinition in generischer Hinsicht besitzt.

3.3.1 Risikoanalyse FunkFahrBetrieb

Mit dem FunkFahrBetrieb (FFB) war in Deutschland ein Betriebsverfahren entwickelt worden, bei dem Funktionalitäten, die heute überwiegend von streckenseitigen Einrichtungen, wie z.B. von Signalen, Stellwerken und Gleisfreimeldeeinrichtungen, wahrgenommen werden, auf das Fahrzeug und in eine Streckenzentrale verlagert worden sind. Die betrieblichen und sicherungstechnischen Vorgänge, wie z.B. Fahrwegzuweisungen, das Ansteuern von Weichen und Bahnübergängen und die Fahrzeugortung (Gleisfreimeldung) wurden funkunterstützt durchgeführt. Im Rahmen des Zulassungsverfahrens war eine Risikoanalyse entsprechend der CENELEC-Normen durchgeführt worden. Der FFB kam anschließend im Jahr 2000 auf einer Pilotstrecke erfolgreich zur Anwendung. Er wird jedoch zurzeit aus strategischen Gründen nicht weiterverfolgt.

FFB-Systemdefinition

Der FFB-Systemdefinition liegt ein hierarchisches Systemmodell zugrunde, in welchem z.B. ein betrachtetes System A nach außen hin gegenüber der Systemumgebung abgegrenzt wird. Das System A besteht selbst aus mehreren Subsystemen, die ihrerseits definierte Systemgrenzen besitzen und wiederum das System A als Umgebung haben. Die Funktionen des Systems A werden durch das Zusammenwirken der Subsysteme realisiert. Die Systemdefinition selbst basiert auf Lastenheften, die bereits die angestrebte Systemarchitektur beschreiben. Die allgemeinen Grundsätze des Funktionierens der Eisenbahn, die mit der Systemlösung „FFB“ umgesetzt werden, werden nicht explizit genannt, sondern gehen über das allgemeine Fachwissen des Fachautors ein. Die auf den Lastenheften aufbauende FFB-Systemdefinition enthält rund 20 Subsysteme, die nach verschiedenen Betrachtungseinheiten strukturiert sind und untereinander in festgelegten Beziehungen stehen (Bild 24).

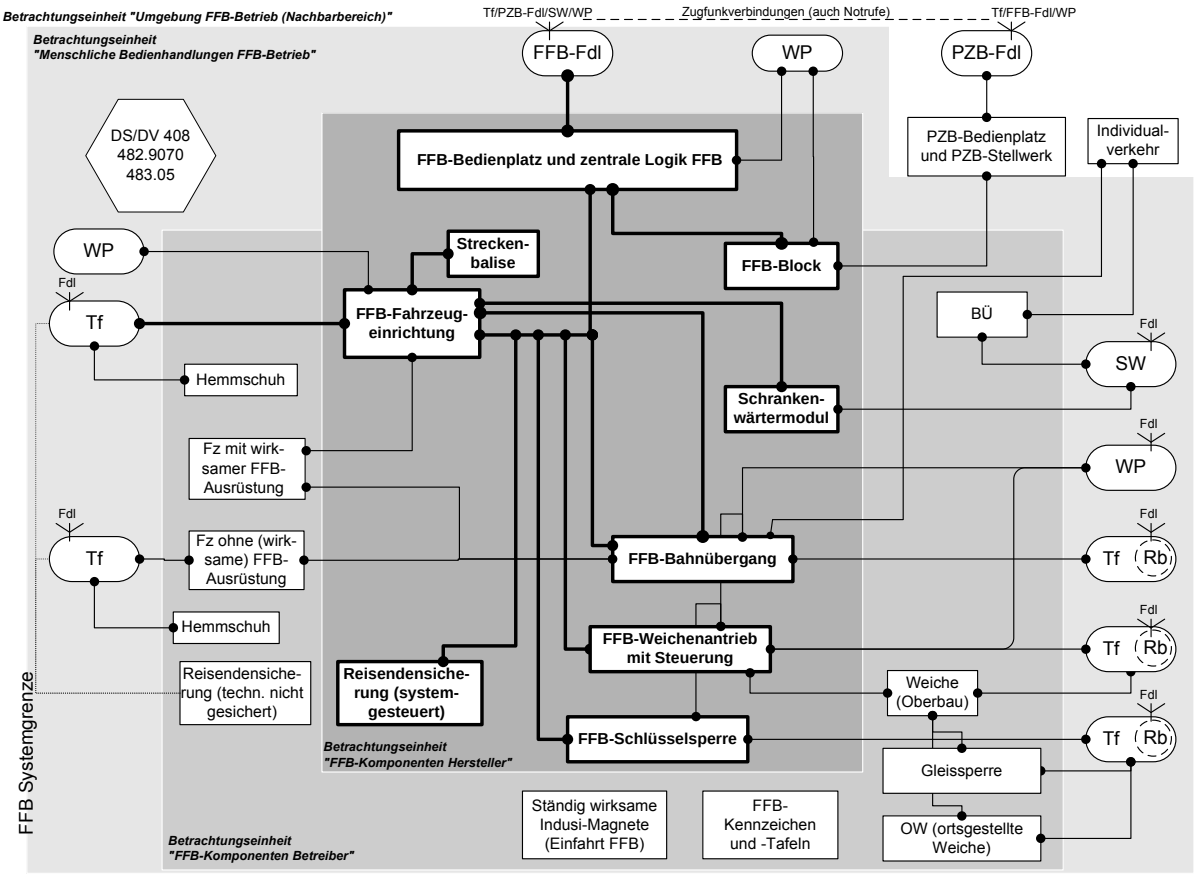


Bild 24: Subsysteme der FFB-Systemarchitektur (Systemdefinition aus [BRA05, S. 70])

Die Funktionalitäten des FFB werden durch die der Systemdefinition zugrunde liegende Systemarchitektur und die Subsysteme ausgedrückt. Es gibt keine von den Subsystemen unabhängige Liste betrieblicher Funktionen, denen die Subsysteme zugeordnet werden. Das bedeutet, dass die in der FFB-Systemdefinition ausgedrückten Funktionalitäten bezogen auf Betriebsverfahren nicht als generisch angesehen werden können, sondern nur bezüglich der möglichen Realisierungen der jeweiligen Subsystemfunktionalitäten.

FFB-Gefährdungsidentifikation

Die Gefährdungen stehen i.d.R. in einem engen Bezug zu den Systemdefinitionen. Dies trifft auch auf die für den FFB identifizierten Gefährdungen zu. Neben der Systemdefinition selbst wurden eine *„allgemeine Checkliste betrieblich gefährlicher Situationen im Bahnbetrieb“* [BRA05, S. 75] und Betriebszenarien aus dem Lastenheft in die Risikoanalyse einbezogen. Beginnend mit einem Brainstormingprozess wurden insgesamt *„40 betrieblich gefährliche Situationen“* [BRA05, S. 74] identifiziert. Zu jeder dieser Situationen wird eine zugehörige „Sicherungsfunktion“ erläutert, die das gefährliche Versagen verhindern soll bzw. auf deren Versagen die betrachtete Situation zurückgehen würde. Gleiches gilt für die im Gefährdungskatalog als *Konsequenzen* bezeichneten Folgen sowie für die Ursachen einer jeden „betrieblich gefährlichen Situation“. Tabelle 6 enthält einen beispielhaften Auszug aus dem Gefährdungskatalog [DB01], der den systemspezifischen Charakter unterstreicht.

Tabelle 6: Auszug aus dem FFB-Gefährdungskatalog [DB01]

FFB-Gefährdungskatalog (beispielhafte Auszüge)	
Betrieblich gefährliche Situation	**Sicherungsfunktion**
FFB-geführter Zug rollt nach Halt an Steigungen mehr als den zulässigen Rückrollweg zurück	*Fahrzeuge dürfen nicht zurückrollen, da der zurückliegende Fahrweg nicht gesichert ist.*
FFB-geführter Zug überschreitet die maximal zulässige Geschwindigkeit bei Fahren auf Sicht.	*FFB hat die Sicherungsfunktion, die Geschwindigkeit im Modus „Fahren auf Sicht" zu überwachen und zu verhindern, dass diese überschritten wird. Fahren auf Sicht kommt zum Einsatz, wenn nicht gesichert ist, dass Gleisabschnitte auf der Strecke frei sind.*
FFB-geführter Zug bekommt unzulässig einen Fahrweg zugewiesen.	*Zusammenstöße werden im FFB durch die Fahrwegverwaltung verhindert. FFB hat die Sicherungsfunktion, Fahrzeugen Fahrwege zuzuweisen und dabei zu verhindern, dass ein Fahrweg zeitgleich mehrfach zugewiesen wird.*
Abgekuppelte / verlorene Zugteile werden nicht erkannt.	*Fahrwegabschnitte dürfen erst als frei gemeldet werden, wenn der Zug in einem folgenden Gleisabschnitt seinen Standort und seine Vollständigkeit gemeldet hat.*
Weiche, die gegen die Spitze befahren wird, läuft unter Rangierfahrt um	*Die Weichensicherung bei Rangierfahrten erfolgt durch den Tf/Rb. Er hat sich über die richtige Stellung der Weichen zu informieren. FFB hat hier die Aufgabe, die Weiche nur umlaufen zu lassen, wenn dieses durch den Tf/Rb angefordert wird.*

Die Analyse der RA FFB führt zu folgenden Ergebnissen (vgl. a. Bild 25):

- Bei der RA FFB handelt es sich um eine vollständig durchgeführte Risikoanalyse, die auf der Architektur des definierten und zu bewertenden Systems beruht.
- Die Systemdefinition wird durch die FFB-Systemarchitektur geprägt. Die auf ihrer Basis identifizierten Gefährdungen sind davon nicht unabhängig und können deshalb bezogen auf Betriebsverfahren nicht als generisch angesehen werden.
- Die formulierten Gefährdungen sind zudem nicht unabhängig von betrieblichen Situationen. Sie werden in dem FFB-Gefährdungskatalog zu recht als *„betrieblich gefährliche Situationen"* und nicht als Gefährdung bezeichnet. In Bild 25 werden sie deshalb auch nicht als „Betriebliche Gefährdung", sondern quasi als Wurzel des Ereignisbaums symbolisiert.

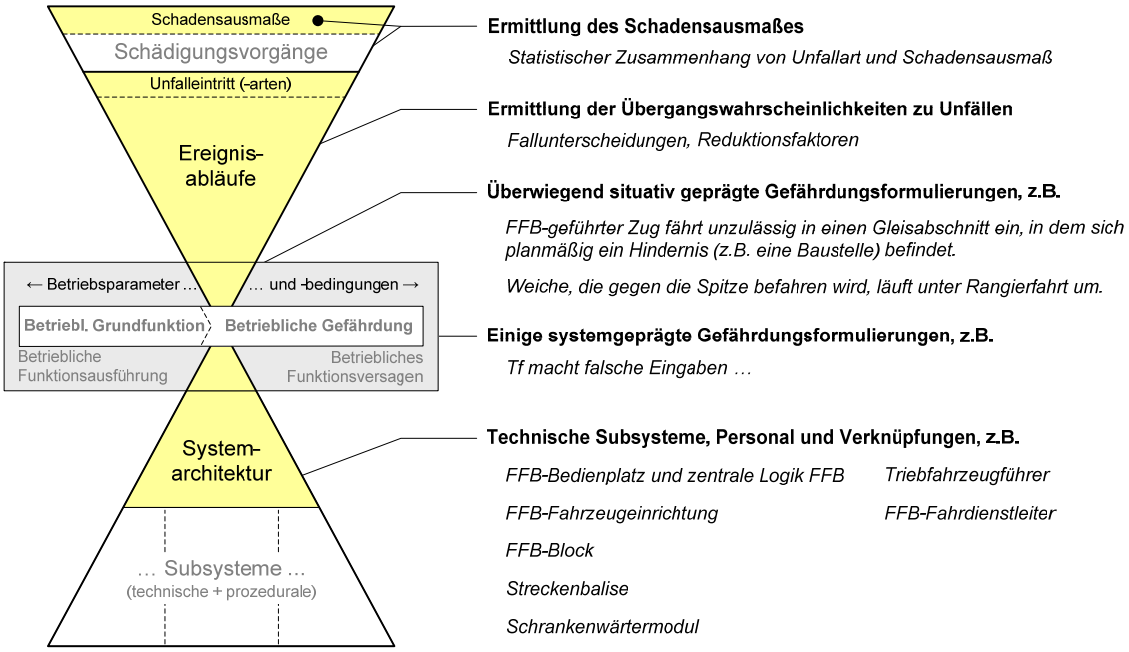


Bild 25: Elemente der RA FFB

Schlussfolgerungen

Der Umfang und die Detaillierungstiefe der Systemdefinition beeinflussen die identifizierten Gefährdungen und die Beschreibung der Funktionen. Im Hinblick auf die angestrebte, für Betriebsverfahren generische funktionale Referenz muss vermieden werden, dass der Systemdefinition weder Realisierungsvorstellungen noch betriebsszenarienspezifische Ausprägungen, wie z.B. die Unterscheidung zwischen Zug- und Rangierfahrten, zugrunde liegen.

3.3.2 Risikoanalyse Elektronisches Stellwerk

Im Gegensatz zur Risikoanalyse FFB ist in der RA ESTW kein umfassendes Betriebsverfahren, sondern der durch das Stellwerk realisierte Teil von Betriebsverfahren untersucht worden. Im Folgenden wird auf die die betrieblichen Funktionen und Gefährdungen betreffenden Aspekte eingegangen. Weitere Details zur RA ESTW finden sich in [BRA05].

Die Systemdefinition umfasst ausgehend von der zu entwickelnden Stellwerksinnenanlage die Schnittstellen zu der Stellwerksaußenanlage, zu Nachbarsystemen und zu technischen Systemen der Umgebung (Bild 26).

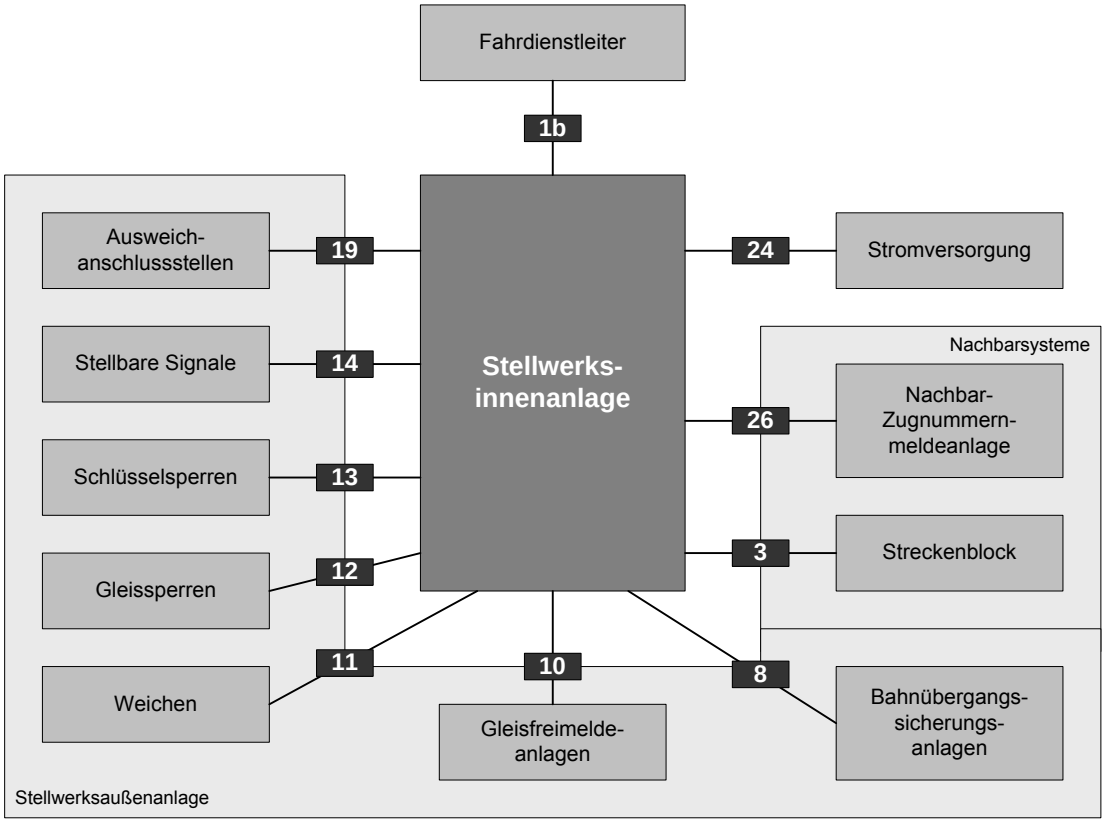


Bild 26: ESTW-Systemarchitektur mit Schnittstellen nach [BRA05, S. 86]

Die Gefährdungen wurden an den definierten Schnittstellen über die Ein- und Ausgaben in bzw. aus der Stellwerksinnenanlage identifiziert. Dabei wurden sowohl in Ausgabe- als auch in Eingaberichtung generische Gefährdungen definiert (Tabelle 7), die später entsprechend der angeschlossen Systeme spezifiziert wurden (Tabelle 8).

Tabelle 7: Generische Schnittstellengefährdungen der ESTW-Innenanlage; [BRA05, S. 88]

Generische Gefährdung	Beschreibung
Falsche Ausgaben werden an die Schnittstelle weitergeben	*Falsche Ausgaben sind durch die Stellwerksinnenanlage falsch ermittelte, inhaltlich veränderte, falsch wiederholte, falsch eingefügte oder ausgelassene Ausgaben, die an der Schnittstelle übergeben werden unter der Voraussetzung, dass das logische Abbild des Zustands des Stellwerks korrekt ist.*
Eingaben über die Schnittstelle werden verfälscht	*Verfälschte Eingaben sind Eingaben, die an der Schnittstelle korrekt anliegen, aber im Verlauf der Weitergabe oder der Verarbeitung durch die Stellwerksinnenanlage verändert, falsch wiederholt, falsch eingefügt oder ausgelassen werden, sodass das logische Abbild des Zustands des Stellwerks verfälscht wird.*

Der nichtfunktionalen Systemdefinition entsprechend wurden die Gefährdungen nicht auf der Basis von Funktionen, sondern auf jener von Informationsflüssen identifiziert. Ferner liegen die identifizierten Gefährdungen nicht auf der Ebene des Betriebsprozesses. In der Tabelle 8

wird dies durch das Beschreiben des Bezugs zur Betriebsprozessebene für die aufgeführten Beispiele unterstrichen.

Tabelle 8: RA-ESTW-Gefährdungskatalog, Bezug zum Betriebsprozess

Auszug aus Liste der Gefährdungen [DB02]		**Bezug zur Betriebsprozessebene**
Gefährdung	**Kommentar**	
Schnittstelle Bedien- und Anzeigesystem (Nr. 1b)		
1b.1b Der Anlagenzustand im KF-Modus wird falsch angezeigt	*Bsp.: Die Lage einer Weiche wird in der gesicherten Anzeige falsch dargestellt, da die Meldung des Stell- und Sicherungssystems inhaltlich verändert wird.*	Die formulierte Gefährdung ist eine Ursache einer übergeordneten betrieblichen Gefährdung im Sinne von „Weiche unerkannt nicht in Solllage“.
1b.2a Die Bedienkommandos der Regelbedienungen werden verfälscht	*Bsp.: Für einen Zug mit Lü wird eine Fahrstraße in ein Gleis eingestellt, das für diese Lü nicht zugelassen ist, weil das Fahrstraßenziel im Kommando verändert wurde.*	Die formulierte Gefährdung ist eine Ursache einer übergeordneten betrieblichen Gefährdung im Sinne von „Konkurrierende LÜ-Fahrt nicht ausgeschlossen“.
Schnittstelle Weiche (Nr. 11)		
11.1 Das falsche Stellkommando wird ausgegeben	*Bsp.: Eine beanspruchte Weiche wird umgestellt, weil das Stellkommando falsch eingefügt wurde.*	Die formulierte Gefährdung ist eine Ursache eine übergeordneten betriebliche Gefährdung im Sinne von „Weiche läuft zur Unzeit um“ sein kann.
11.2 Die Weichenmeldung wird verfälscht	*Die Weichenmeldung weicht von dem tatsächlichen Weichenzustand ab.* *Bsp.: Die Weiche liegt in falscher Lage, weil die Lagemeldung inhaltlich verändert wurde.*	Die formulierte Gefährdung ist eine Ursache einer übergeordneten betrieblichen Gefährdung im Sinne von „Weiche unerkannt nicht in Solllage“.

Es ist festzustellen, dass weder die identifizierten Gefährdungen noch die erläuternden Kommentare auf der betrieblichen Prozessebene liegen. Aus betrieblicher Sicht sind sie Ursachen für betriebliche Gefährdungen. Die gesuchten betrieblichen Gefährdungen und Funktion liegen somit auf einer höheren Systemebene als die identifizierten Schnittstellengefährdungen (Bild 27). Hierin begründet sich auch, dass mehrere der identifizierten Schnittstellengefährdungen zu derselben betrieblichen Gefährdung führen.

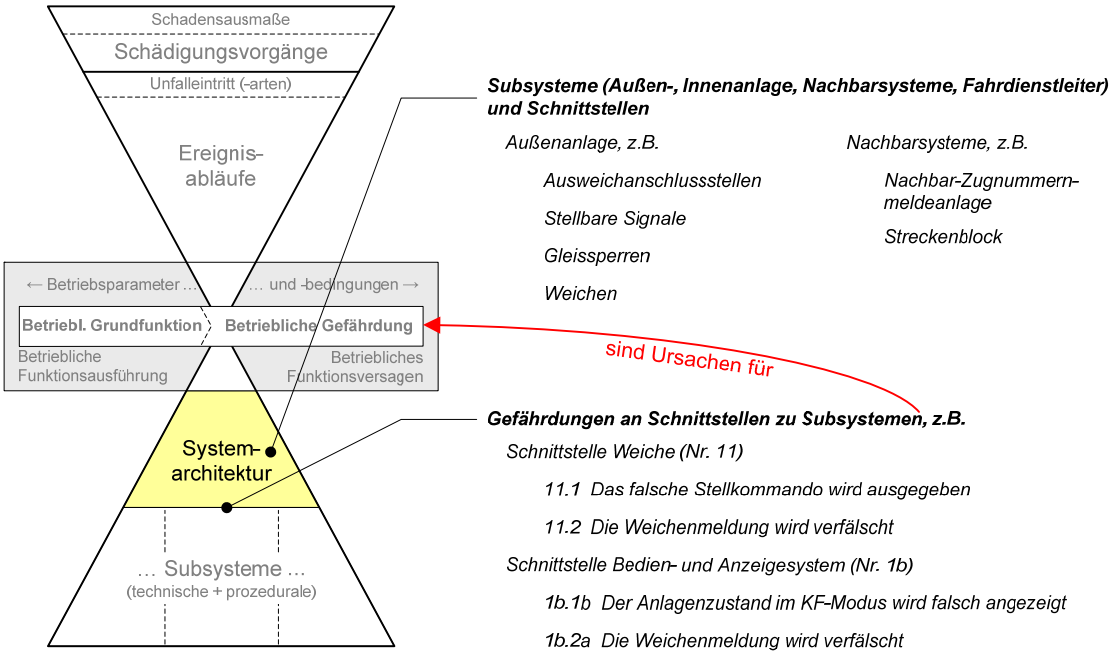


Bild 27: Gefährdungen in RA ESTW sind Ursachen für betriebliche Gefährdungen

Schlussfolgerungen

Die Risikoanalyse ESTW ist auf einer unterhalb der Betriebsverfahren liegenden Systemebene durchgeführt worden. Sie enthält deshalb weder Definitionen betrieblicher Funktionen noch enthält die Gefährdungsliste die entsprechenden betrieblichen Gefährdungen. Wollte man auf der Basis der RA ESTW betriebliche Funktionen quasi rekursiv aus den identifizierten Gefährdungen ableiten, müsste dazu ein System auf der betrieblichen Ebene definiert werden, in dessen Funktionalitäten das ESTW einzuordnen wäre.

3.3.3 Risikoanalyse ETCS (Pilotanwendung)

Im Rahmen der Risikoanalyse für die ETCS-Pilotanwendung wurde ein betrieblich-funktionaler Ansatz verfolgt, der Funktionen oberhalb herstellerspezifischer Systemarchitekturen definiert. Dazu sind die für eine Zugfahrt zu realisierenden Funktionen definiert worden [LHB03]. Die zur Herstellerseite hin vorgenommene Begrenzung des Betrachtungsraums führt zu einer abstrakteren Funktionsliste, die frei von herstellerspezifischen Prägungen ist. Auf Basis dieser Liste wurden Gefährdungen funktional abgeleitet.

Der durch ETCS abgedeckte Funktionsbereich deckt nur einen Teilbereich der Betriebsverfahren ab. Die in [LHB03] aufgeführten Funktionen sind nicht nur unabhängig von Herstellerspezifika, sondern auch kaum durch das betrachtete System ETCS geprägt. Die Autoren der Veröffentlichung berichten, dass sich aussagekräftige Definitionen für Funktionen erst ab einer „gewissen Detaillierung“ ergeben und auch nur bis zu einer Ebene hinab möglich sind, „weil dann bereits Lösungen oder betriebliche Abläufe beschrieben werden müssten“. Daraus ist zu schließen, dass sich die betrieblichen Funktionen auch bei einer generischen

Betrachtungsweise in einem gewissen Maße hierarchisch gliedern lassen und zu funktionalen Gruppen zusammenfassen lassen können. Dies deckt sich vom Ansatz her mit dem hierarchisch gegliederten Aufbau der prEN 15380-4.

3.4 Zusammenfassung der Analyseergebnisse

Die durchgeführten Analysen führen bezogen auf die Betrachtungsebene von Betriebsverfahren zu folgenden Ergebnissen:

- Die in der prEN 15380-4 enthaltene Funktionsliste ist bislang die einzige Liste, die der Funktionen in mehreren Stufen hierarchisch gliedert werden. Sie ist jedoch auf Fahrzeuge bezogen und enthält nur im Sinne von Schnittstellen Funktionen, die einen Bezug zu Funktionen haben, die dem Bereich der Betriebsverfahren zuzurechnen sind. Eine allgemeine funktionale Beschreibung des Eisenbahnsystems, das in der CENELEC-Norm EN 50127 (Railway Applications – guide to the specification of a guided transport system) realisiert werden sollte, gilt als gescheitert [BEP08, S. 44].
- Die in der prEN 15380-4 enthaltenen Funktionen decken auch unter Berücksichtigung der in [BEP08] ergänzten Funktionen nur einen Teil des Funktionsraums der Betriebsverfahren ab. Gleiches gilt für die im Rahmen der RA ETCS (Pilotstrecke) erstellte Funktionsliste.
- Das Ableiten von Funktionen aus einer *„allgemeine Checkliste betrieblich gefährlicher Situationen im Bahnbetrieb“* [BRA05, S. 75], wie z.B. der IEC 62267-2 ist eine prinzipielle Möglichkeit, Funktionen zu definieren, die von Betriebsverfahren zu erfüllen sind. Zu jeder relevanten Gefährdung wird eine Funktion definiert, mit der sie beherrscht werden soll. Durch die mit den entsprechenden Systemdefinitionen beschriebenen Architekturen können die so im Prinzip einzeln abgeleiteten Funktionen dem betrachteten System und seinen Subsystemen zugeordnet und untereinander in einen Zusammenhang gebracht werden. Dieses Vorgehen hat sich beim Durchführen von Risikoanalysen bewährt. Im Gegensatz zu diesen Unikaten bedingt das Definieren eines generischen Referenzsystems jedoch den Verzicht auf vergleichbare Systemarchitekturen. Dies erschwert die Einordnung der Funktionen, so dass zwar eine Liste einzeln abgeleiteter Funktionen erwartet werden darf, ohne aber die im System Betriebsverfahren enthaltenden funktionalen und hierarchischen Wirkungszusammenhänge in einem für ein generisches Referenzsystem ausreichenden Maß abzubilden.
- Die im Rahmen von Risikoanalysen entstandenen Funktions- und Gefährdungslisten sind systemspezifische Unikate. Die in den Risikoanalysen enthaltenen Definitionen und Beschreibungen sind bezogen auf Betriebsverfahren nicht generisch formuliert worden, sondern sind durch die jeweiligen Systemarchitekturen geprägt. Eine unmittelbare Ableitung eines generischen Referenzsystem auf Basis dieser Listen ist problematisch, da zum einen stark von der vorgegeben Lösung abstrahiert werden muss und zum anderen

die betrachteten Systeme i.d.R. nicht den vollen Funktionsumfang der Betriebsverfahren abdecken.

Fazit

Für den Bereich der Betriebsverfahren gibt es bislang keine umfassende Liste von betrieblichen Funktionen, die als generisch angesehen und unmittelbar als Grundlage für ein generisches Referenzsystem verwendet werden kann. Die vorhandenen Listen sind i.d.R. systemspezifisch geprägt, decken den Funktionsumfang von Betriebsverfahren nur teilweise ab, entstammen in ihrem Kern anderen Anwendungsgebieten und/oder lassen keine für eine generische Referenz für Betriebsverfahren ausreichende Strukturierung erwarten. Ihre unmittelbare Anwendung zum Definieren der generischen Referenz wird angesichts der zentralen Bedeutung der Betriebsverfahren für die Sicherheit der Eisenbahn als problematisch angesehen. Da sie sich jedoch im Rahmen ihrer ursprünglichen Anwendungen, wie z.B. in Risikoanalysen bewährt haben, sollten sie zur späteren Verifizierung des generischen Referenzsystems herangezogen werden.

Die für das Erarbeiten eines generischen Referenzsystem für Betriebsverfahren interessanten Ansätze bieten die prEN 15380-4 und das bei der RA ETCS (Pilotstrecke) gewählte Vorgehen. Die Norm wegen des hierarchischen Aufbaus und die Risikoanalyse wegen ihres betrieblich-funktionalen Ansatzes. Beide Ansätze decken jedoch nur einen Teil der Betriebsverfahren ab, der zudem überwiegend technisch geprägt ist. Es ist deshalb zu erwarten, dass beim Erarbeiten eines generischen Referenzsystems noch höhere Anforderungen sowohl an das Abstraktionsvermögen als auch an die realisierungsunabhängige Beschreibung zu stellen sind. Im Kapitel 4 wird als Grundlage für seine Erarbeitung ein Vorgehen entwickelt, das das Erfüllen dieser Anforderungen beginnend vom Festlegen einer als Betrachtungsraum dienenden Systemdefinition, über das Abgrenzen funktionaler Strukturen, dem Definieren hierarchisch gegliederter Funktionen bis hin zur Identifizierung von Funktionen unterstützen soll.

4 Vorgehen zum Definieren generischer Funktionen und Gefährdungen

Die im Kapitel 3 durchgeführte Analyse der vorhandenen Funktions- und Gefährdungslisten hat ergeben, dass diese für spezifische Anwendungen erstellt worden sind und es bislang weder eine Funktions- noch eine Gefährdungsliste gibt, die für die Betriebsverfahren spurgeführter Verkehrssysteme als generisch angesehen werden können. Ein wesentlicher Grund ist in der Berücksichtigung vorgegebener Systemstrukturen zu sehen, die im Folgenden auch als Systemarchitekturen bzw. in verkürzter Form als Architekturen bezeichnet werden. Im Hinblick auf die sehr heterogenen Gestaltungsmöglichkeiten für Betriebsverfahren ist die Unabhängigkeit von der Systemarchitektur als die zentrale Voraussetzung für die Definition betriebsverfahrensübergreifender generischer Funktionen anzusehen.

Die Analyse der Funktionsliste aus dem Fahrzeugbereich hat zudem Mängel offenbart, die auf dem zum Teil stichwortartigen Formulieren der Funktionen und auf der Benennung von spezifischen Begriffen von Verfahren und Einrichtungen beruhen. Als problematisch ist anzusehen, dass nicht immer zwischen den zugrunde liegenden Handlungen und Vorgängen und dem Funktionszweck unterschieden werden kann. Die für eine generische Definition erforderliche Unabhängigkeit von Systemarchitekturen würde diese Problematik u.U. verschärfen, da ihretwegen auf einige das Verständnis erleichternde Anhaltspunkte verzichtet werden muss.

Im Abschnitt 4.1 werden die Grundlagen für eine architekturunabhängige generische Systemdefinition geschaffen. Im Abschnitt 4.2 wird ein Vorschlag entwickelt, wie mit sprachlichen Mitteln nicht nur die Aussagekraft von Funktionsdefinitionen verbessert, sondern auch der generische Anspruch gewahrt werden und darauf aufbauend auch generische Gefährdungen identifiziert werden können (4.3). Als Ergänzung zur Definition werden in 4.4 allgemeine Funktionsgrundtypen definiert, die sich an der modifizierten Sanduhr orientierten. Um ein einheitliches Vorgehen beim Definieren betrieblicher Funktionen und dem integrierten Identifizieren der Gefährdungen zu unterstützen, werden in 4.5 Formulare geschaffen, die zudem als Eingabemasken für eine generische Funktionsdatenbank dienen können.

4.1 Architekturunabhängige generische Systemdefinition

In Anlehnung an das in Risikoanalysen übliche Vorgehen ist davon auszugehen, dass auch die Definition betrieblicher Funktionen einer Art Systemdefinition bedarf, um den Betrachtungsraum gegenüber seiner Umwelt abzugrenzen. Sowohl das zu betrachtende System als auch die Systemgrenzen und Schnittstellen (Terminatoren) müssen festgelegt werden. Um dem Anspruch zu genügen, die definierten Funktionen mögen für alle spurgeführten Verkehrssysteme gelten, dürfen jedoch im Vergleich zu dem bei konkreten Anwendungsfällen üblichen Umfang bestimmte Angaben gar nicht oder nur in einem reduzierten Umfang

gemacht werden. Bezogen auf den betrachteten Prozess müssen folglich auch die Terminatoren generisch definiert werden, d.h. auch sie müssen unabhängig von der Realisierung des betrachteten Prozesses Gültigkeit besitzen. Der Begriff „Systemdefinition“ ist vor diesem Hintergrund zu beleuchten. Er ist ggf. so zu modifizieren, dass er einerseits den Anforderungen hinsichtlich der angestrebten Generik gerecht wird, andererseits aber auch nicht in einem Widerspruch zu den im Anwendungsgebiet gültigen Normen steht.

Der Begriff der Systemdefinition sowie sein inhaltlicher Umfang werden in verschiedenen normativen Vorgaben festgelegt. Die im Eisenbahnwesen einschlägigen Vorgaben werden im Abschnitt 4.1.1 in ihren Grundzügen erläutert. Sie werden im Abschnitt 4.1.2 insoweit modifiziert, wie es für das Erstellen architekturunabhängiger generischer Systemdefinitionen erforderlich ist. Damit soll der Bezug zu den etablierten Vorgaben erhalten bleiben.

4.1.1 Normative Vorgaben

Für den Begriff „Systemdefinition“ sind die Normen EN 50126 und EN 50129 sowie die von der European Railway Agency (ERA) herausgegebene *Recommendation on the 1st set of Common Safety Methods* [ERA07] maßgebend. Sie bilden die Grundlagen für das Führen von Sicherheitsnachweisen.

4.1.1.1 EN 50126 und EN 50129

Die Definition eines Systems und die Identifizierung von Gefährdungen sind Schritte, die Bestandteile des in der EN 50129 beschriebenen Sicherheitsanalyseprozesses sind. Dieser in der Norm in Form einer Sanduhr dargestellte Prozess zielt darauf ab, für Gefährdungen tolerierbare Gefährdungsraten (THR) zu ermitteln, die von einem bestimmten zu entwickelnden System „beherrscht“ werden müssen.

Der Sicherheitsanalyseprozess (Bild 28) ist darauf angelegt, den gesamten Entwicklungsprozess eines konkreten Produkts zu begleiten. „Konkret“ bedeutet in diesem Zusammenhang, dass bereits Vorstellungen über die Einsatzbedingungen und einen grundsätzlichen strukturellen Aufbau des Systems existieren. Letzteres kann bereits in einer Aufteilung der Aufgaben zwischen Mensch und Technik zum Ausdruck kommen; es kann aber, wie am Beispiel der Risikoanalyse FunkFahrBetrieb im Abschnitt 3.3.1 gezeigt worden ist, auch noch detaillierter ausfallen.

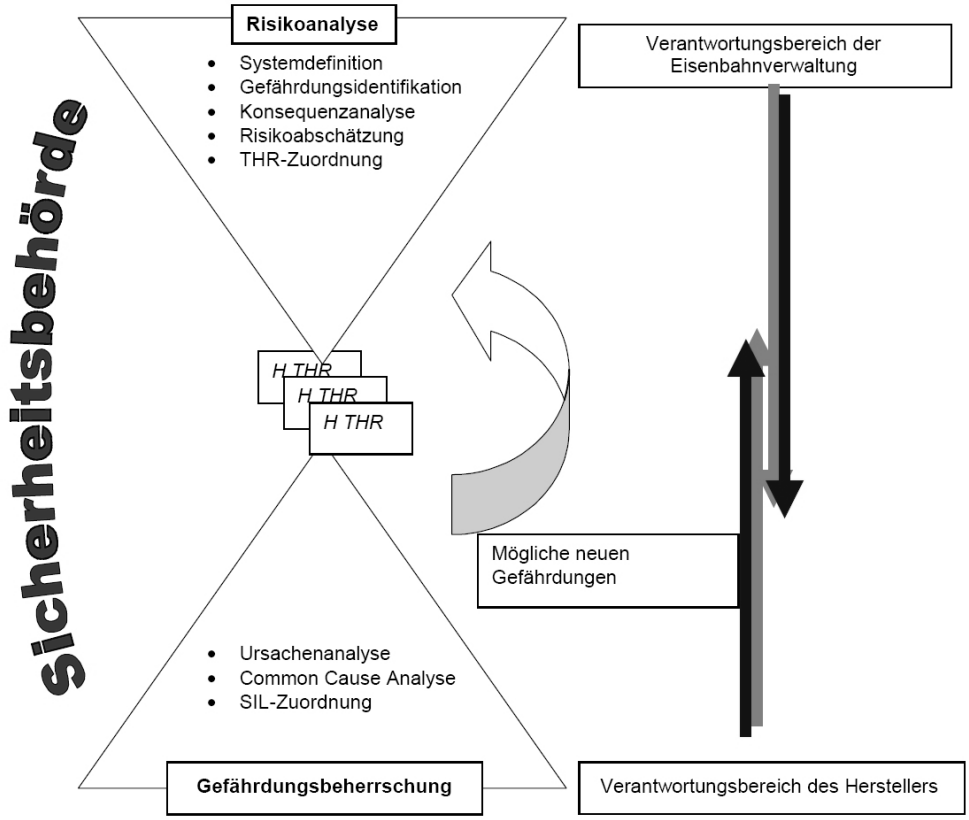


Bild 28: Darstellung des Sicherheitsanalyseprozesses in [EN 50129]

Der Betrachtungsweise der EN 50129 folgt auch die Norm EN 50126, in der ein System als eine „*Komposition von Subsystemen und Komponenten*“ definiert wird*, „die zur Gewährleistung der geforderten Funktionalität in geregelter Form miteinander verbunden sind“.* Die Funktionalität des Systems wird in dieser Norm *„den Subsystemen und Komponenten eines Systems zugeschrieben“.* Ferner würden sich das Verhalten und der Zustand des Systems *„mit einer Änderung der Funktionalität eines Subsystems oder einer Komponente“* ändern. Mit der Zuschreibung der Funktionalität[24] zu den Subsystemen und Komponenten stellt die Norm folglich einen engen Bezug zwischen der Funktionalität und Subsystemen bzw. Komponenten her und rückt diesen in den Vordergrund.

Fazit

Den Normen EN 50126 und EN 50129 liegt die Vorstellung zugrunde, dass insbesondere für komplexere Systeme bereits Vorüberlegungen zu der Struktur der Subsysteme und zu den Komponenten eines Systems vorliegen, anhand derer die Funktionalität des Systems beschrieben werden kann. Das Beispiel der Risikoanalyse FunkFahrBetrieb zeigt, welche Umfänge derartige Systemarchitekturen im Falle von Betriebsverfahren annehmen können.

[24] Funktionalität: Fähigkeit eines Produkts, eine bestimmte Aufgabe oder Menge von Aufgaben zu lösen.

Sollen aber, wie in dieser Arbeit angestrebt, die durch unterschiedlich strukturierte Betriebsverfahren realisierten betrieblichen Funktionen gemeinsam als generische Funktionen definiert werden, ist eine Entkopplung der Systemdefinition und der Funktionalität des Systems von seinen internen Strukturen, d.h. von den möglichen Subsystemen, Komponenten und deren Verknüpfungen, notwendig. Im Abschnitt 2.4 wird deshalb bereits der Begriff „imaginäres System generischer Funktionen“ verwendet, der durch die vorstehenden Überlegungen bestätigt und konkretisiert wird.

4.1.1.2 CSM-Recommendation der ERA

Die European Railway Agency (ERA) empfiehlt in der von ihr herausgegebenen *Recommendation on the 1st set of Common Safety Methods* [ERA07], welche Punkte eine Systemdefinition umfassen soll. Die Empfehlung liegt in englischer Sprache vor; da aber absehbar ist, dass die Anwendung dieser Empfehlungen auf eine generische Systemdefinition der inhaltlichen Anpassung und Weiterentwicklung im Rahmen dieser deutschsprachigen Arbeit bedarf, werden die Anforderungen der ERA zur späteren Weiterverwendung sinngemäß ins Deutsche übersetzt. Sinngemäße Übersetzungen erlauben eine sprachliche und damit inhaltliche Präzisierung; sie bergen aber auch die Gefahr einer ungewollten Interpretation in sich. Der inhaltlichen Nachvollziehbarkeit halber werden die deutschen Übersetzungen in Tabelle 9 den englischsprachigen Originalformulierungen gegenübergestellt.

Tabelle 9: Übersetzung der ERA-Anforderungen an eine Systemdefinition

Anforderungen gemäß [ERA07]	**Deutsche Übersetzung (sinngemäß)**
The system definition should address at least the following issues:	Die Systemdefinition sollte mindestens folgende Punkte umfassen:
(a) definition of system objective, e.g. intended purpose;	Definition des Systemziels, z.B. der beabsichtigte Einsatzzweck des Systems;
(b) definition of system functions and elements, where relevant (including e.g. human, technical and operational elements);	Definition der Systemfunktionen und, sofern sachdienlich, von Systemelementen, die z.B. menschlicher, technischer und betrieblicher Natur sein können;
(c) definition of system boundary including other interacting systems;	Definition der Systemgrenze einschließlich der mit dem System in Beziehung stehenden Nachbarsysteme;
(d) definition of physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;	Definition der physikalischen Schnittstellen zu den mit dem System in Beziehung stehenden Nachbarsystemen sowie der funktionalen Ein- und Ausgabe-Schnittstellen;
(e) definition of system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);	Definition der Einsatzbedingungen des Systems, wie z.B. Kraft- und Wärmeflüsse, Erschütterungen, Vibrationen, elektromagnetische Beeinflussungen und betriebliche Verwendung;

Anforderungen gemäß [ERA07]	Deutsche Übersetzung (sinngemäß)
(f) definition of the existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process;	Definition der vorhandenen Sicherheitsvorkehrungen und Definition der im Risikobewertungsprozess in [einem oder mehreren] Iterationsschritten identifizierten Sicherheitsanforderungen;
(g) definition of the assumptions which shall determine the limits for the risk assessment.	Definition der Annahmen, mit denen der Betrachtungsumfang des Risikobewertungsprozesses festgelegt wird.

Fazit

Die CSM-Recommendation der ERA steht nicht im Widerspruch zu den Normen EN 50126 und EN 50129. In ihr wird das Vorgehen zum Erstellen und die Art und Weise einer Systemdefinition konkreter als in den Normen EN 50126 und EN 50129 beschrieben. Aber ihr liegt, wie die Anforderung (b) zeigt, ebenfalls die Vorstellung zugrunde, dass insbesondere für komplexere Systeme bereits Ideen oder Kenntnisse über eine Systemarchitektur vorliegen werden oder Vorstellungen existieren, anhand derer die Funktionalität des Systems beschrieben werden kann. Dieser realisierungs-, d.h. anwendungsnahe Ansatz der CSM-Recommendation kommt auch in Teilen der Anforderungen (e), (f) und (g) zum Ausdruck. Insofern muss, um für in unterschiedlich strukturierten Betriebsverfahren realisierte betriebliche Funktionen gemeinsame generische Funktionen definieren zu können, ebenfalls eine Entkopplung der Funktionalität des Systems von den systeminternen Strukturen sichergestellt werden.

4.1.2 Anforderungen für eine architekturunabhängige generische Systemdefinition

4.1.2.1 Ableitung der Anforderungen

Wie im Abschnitt 4.1.1 gezeigt werden konnte, enthält die CSM-Recommendation der ERA eine ausführliche Sammlung von Anforderungen an Systemdefinitionen im europäischen Eisenbahnwesen. Es wurde aber auch deutlich, dass einige dieser Anforderungen auf die Beschreibung systeminterner Strukturen abzielen, um anhand dieser Strukturen Systemfunktionen zu definieren. Dies steht im Widerspruch zu dem in dieser Arbeit verfolgten Ziel, Funktionen unabhängig von ihrer technischen Realisierung und damit auch unabhängig von Systemarchitekturen beschreiben zu wollen. Gleiches gilt für die Einsatzbedingungen und –bereiche, die ihrerseits sehr unterschiedlich ausfallen können. Deshalb werden in der Tabelle 10 die Anforderungen der CSM-Recommendation dahingehend modifiziert, dass sie für systemstrukturunabhängige generische Systemdefinitionen Anwendung finden können. Dazu werden die einzelnen Anforderungen entsprechend erörtert und neue Formulierungen abgeleitet.

Tabelle 10: Anforderungsableitung für architekturunabhängige generische Systemdefinitionen

Anforderungen gemäß [ERA07] (deutsche Übers.)		**Erörterung**	**Abgeleitete Anforderungen**
(a)	*Definition des Systemziels, z.B. der beabsichtigte Einsatzzweck des Systems;*	Diese Anforderung kann auch unter generischen Gesichtspunkten erfüllt werden, da sie zur Beschreibung keiner Struktur- oder sonstigen Realisierungsangaben bedarf.	Definition des Systemziels in allgemeingültiger, realisierungsunabhängiger Form, z.B. der beabsichtigte Einsatzzweck des Systems;
(b)	*Definition der Systemfunktionen und, sofern sachdienlich, von Systemelementen, die z.B. menschlicher, technischer und betrieblicher Natur sein können;*	Eine Funktion ist generisch, solange sie keine Bezüge zu einer von mehreren möglichen Systemstrukturen und Funktionsrealisierungen hat; deshalb ist die Angabe von „Systemelementen“ i.S. von Subsystemen oder Komponenten aus generischer Sicht unzulässig.	Definition der Systemfunktionen ohne Bezug auf Systemarchitekturen, Komponenten oder sonstige Realisierungen;
(c)	*Definition der Systemgrenze einschließlich der mit dem System in Beziehung stehenden Nachbarsysteme;*	Die Definition kann im Prinzip übernommen werden; allerdings sollte, um physikalisch geprägten Systemgrenzen vorzubeugen, der Hinweis „funktional“ aufgenommen werden. Die Definition einer materiellen Grenze ist nur dann angebracht, wenn es sich um eine allgemeingültige Grenze handelt, wie z.B. zwischen Fahrzeug und Umgebung (Fahrzeugumgrenzung und Lichtraum)	Definition der funktionalen Systemgrenze einschließlich der mit dem System in Beziehung stehenden funktionalen Nachbarsysteme; Definition physikalischer Grenzen nur, wenn sie allgemeingültig mit funktionalen Grenzen zusammenfallen;
(d)	*Definition der physikalischen Schnittstellen zu den mit dem System in Beziehung stehenden Nachbarsystemen sowie der funktionalen Ein- und Ausgabe-Schnittstellen;*	Die Definition physikalischer Schnittstellen setzen die Kenntnis oder zumindest Vorstellungen voraus, welcher Art die Nachbarsysteme, die Umgebung sowie die Architektur des Systems sind bzw. sein könnten. Generisch können deshalb nur die funktionalen Ein- und Ausgabeschnittstellen definiert werden.	Definition der funktionalen Ein- und Ausgabe-Schnittstellen zu den mit dem System in Beziehung stehenden Nachbarsystemen; Definition physikalischer Schnittstellen nur, wenn sie allgemeingültig mit funktionalen Schnittstellen zusammenfallen

Anforderungen gemäß [ERA07] (deutsche Übers.)		Erörterung	Abgeleitete Anforderungen
(e)	*Definition der Einsatzbedingungen des Systems, wie z.B. Kraft- und Wärmeflüsse, Erschütterungen, Vibrationen, elektromagnetische Wechselwirkungen und betriebliche Verwendung;*	Diese Angaben können bei einer auf unterschiedliche Bahnen bezogene generische Betrachtungsweise nicht gemacht werden. Sie müssen später im konkreten Vorhaben einbezogen werden.	Entfällt; Angabe erst bei konkretem Vorhaben bearbeitbar
(f)	*Definition der vorhandenen Sicherheitsvorkehrungen und Definition der im Risikobewertungsprozess in [einem oder mehreren] Iterationsschritten identifizierten Sicherheitsanforderungen;*	Diese Angaben können bei einer auf unterschiedliche Bahnen bezogene generische Betrachtungsweise nicht gemacht werden. Sie müssen später im Einzelfall einbezogen werden.	Entfällt; Angabe erst bei konkretem Vorhaben bearbeitbar
(g)	*Definition der Annahmen, mit denen der Betrachtungsumfang des Risikobewertungsprozesses festgelegt wird.*	Sofern die Annahmen Punkte berühren, die unter (e) und (f) als konkrete Vorhaben zu betrachten sind, sind sie nicht möglich; haben sie jedoch einen für alle Bahnen geltenden Charakter, können sie gemacht werden. Da die Bewertung des Risikos eine Quantifizierung erfordert, dies aber nur bei konkreten Vorhaben möglich ist, wird der Begriff „Risikobewertungsprozess“ nicht verwendet.	Definition allgemeingültiger Annahmen, mit denen der Betrachtungsumfang des Systemdefinitionsprozesses festgelegt wird.

4.1.2.2 Reihung der Anforderungen

Die bei architekturunabhängigen generischen Systemdefinitionen bestehende Notwendigkeit, nicht nur auf die Beschreibung von Funktionsrealisierungen verzichten zu müssen, sondern auch keine Systemarchitekturen angeben zu können, bedeutet für die Erarbeitung der Systemdefinition den Verlust entsprechender konkretisierender Anhaltspunkte. Zum Beispiel kann ein solches System ohne Bezüge zu einer Systemarchitektur nicht mehr von „innen heraus“ definiert werden. Die Systemdefinition wird deshalb auf den mit dem System in Beziehung stehenden Nachbarsystemen und den entsprechenden funktionalen Schnittstellen aufbauen müssen. Das „System“ kann quasi nur von außen her definiert werden. Die in Tabelle 10 neu formulierten Anforderungen werden deshalb i.d.R. in einer anderen Reihenfolge, d.h. von „außen nach innen“ abzuarbeiten sein. Aus diesem Grunde werden sie in der Tabelle 11 in entsprechender Reihenfolge sortiert. Die Sortierung ist in die drei

Abschnitte *Allgemeine Definitionen*, *Äußere Definitionen* und *Innere Definitionen* gegliedert. Ferner werden die Bezüge zu den ursprünglichen Anforderungen der CSM-Recommendation angegeben.

Tabelle 11: Anforderungen für eine architekturunabhängige generische Systemdefinition

Eine architekturunabhängige generische Systemdefinition sollte folgende Punkte beinhalten:		**Bezug zur CSM-Rec. [ERA07]**
(1) Allgemeine Definitionen		
(1.1)	Definition des Systemziels in allgemeingültiger, realisierungsunabhängiger Form, z.B. der beabsichtigte Einsatzzweck des Systems;	Chapter III, Article 6, 2. (a)
(1.2)	Definition allgemeingültiger Annahmen, mit denen der Betrachtungsumfang des Systemdefinitionsprozesses festgelegt wird.	Chapter III, Article 6, 2. (g)
(2) Äußere Definitionen		
(2.1)	Definition der funktionalen Systemgrenze einschließlich der mit dem System in Beziehung stehenden funktionalen Nachbarsysteme;	Chapter III, Article 6, 2. (c)
(2.2)	Definition physikalischer Grenzen nur, wenn sie allgemeingültig mit funktionalen Grenzen zusammenfallen;	
(2.3)	Definition der funktionalen Ein- und Ausgabe-Schnittstellen zu den mit dem System in Beziehung stehenden Nachbarsystemen;	Chapter III, Article 6, 2. (d)
(2.4)	Definition physikalischer Schnittstellen nur, wenn sie allgemeingültig mit funktionalen Schnittstellen zusammenfallen.	
(3) Innere Definitionen		
(3.1)	Definition der Systemfunktionen ohne Bezug auf Systemarchitekturen oder sonstige Realisierungen zu nehmen.	Chapter III, Article 6, 2. (b)

Aus den in der Tabelle 11 enthaltenen Anforderungen ergibt sich eine grundsätzliche Struktur zwischen dem zu betrachtenden funktionalen System, seinen Nachbarsystemen und den abgrenzenden Schnittstellen (Bild 29).

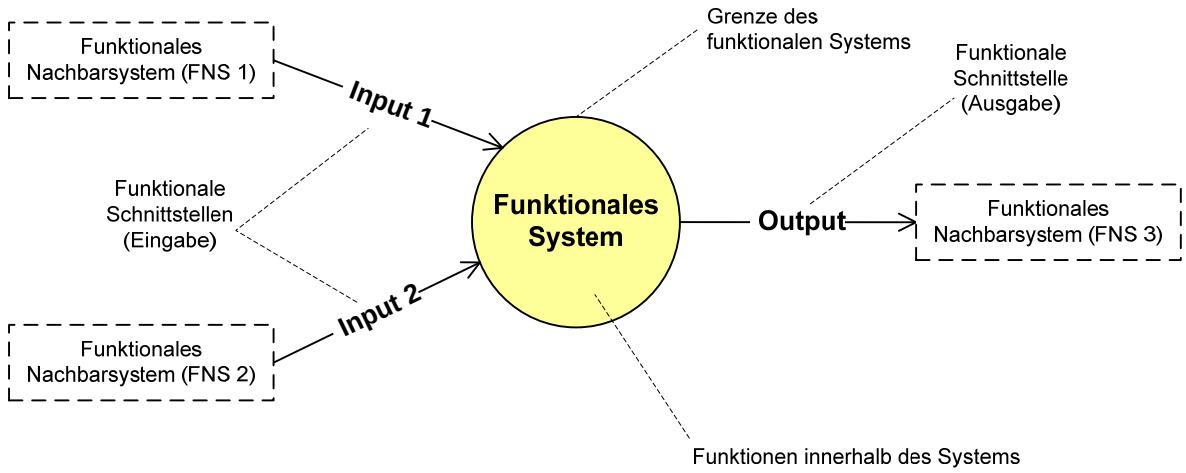


Bild 29: Beispielhafte Struktur der Definition eines Funktionalen Systems

Einen besonderen Stellenwert bei der Abgrenzung des zu betrachtenden Systems nehmen In- und Output ein. Durch sie wird definiert, was das System zu leisten hat (Output) und was es nicht leisten, sondern von anderen Systemen übernehmen soll (Input). Wer oder was diese Inputs liefert, ist bei generischer Betrachtungsweise im Prinzip unerheblich. Deshalb könnte theoretisch die Angabe der Nachbarsysteme entfallen und die Abgrenzung allein durch die Angaben zu den In- und Outputs vorgenommen werden. Im Hinblick auf anschauliche Darstellung erscheint es jedoch angebracht zu sein, auch die Nachbarsysteme zu benennen.

4.1.3 Beiträge zum Sicherheitsanalyseprozess gemäß EN 50129

Wie in den vorstehenden Abschnitten gezeigt werden konnte, kann eine architekturunabhängige generische Systemdefinition prinzipbedingt nicht alle in der CSM-Recommendation aufgeführten Anforderungen erfüllen. Gleiches ist für den Sicherheitsanalyseprozess gemäß EN 50129 zu erwarten, für den die Systemdefinition die Ausgangsbasis bildet. In der Tabelle 12 wird erläutert, zu welchen der weiteren im Sicherheitsanalyseprozess („Sanduhr", Bild 28) durchzuführenden Schritten eine architekturunabhängige Systemdefinition beitragen kann.

Tabelle 12: Mögliche Beiträge architekturunabhängiger generischer Systemdefinitionen zum Sicherheitsanalyseprozess

Schritt gemäß „Sanduhr" [EN 50129]		**Beitrag architekturunabhängiger generischer Systemdefinition**
Risikoanalyse („oberes Dreieck")	*Systemdefinition*	Die architekturunabhängige generische Systemdefinition bildet einen auf generischen Funktionen beruhenden Rahmen, auf den später bei jeder Einzelfallbetrachtung entsprechende Subsysteme und Komponenten referenziert werden können. Der Rahmen stellt für alle Systemarchitekturen und –realisierungen eine einheitliche Betrachtungs- und Vergleichsebene dar.
	Gefährdungsidentifikation	Auf der Basis definierter Funktionen können Gefährdungen identifiziert werden. Sind die Funktionen generisch definiert, können auch die daraus abgeleiteten Gefährdungen als generisch angesehen werden. Die in konkreten Vorhaben auf Systemarchitekturen und –realisierungen bezogenen Gefährdungen sind Ursachen der generischen Gefährdungen.

Schritt gemäß „Sanduhr“ [EN 50129]		**Beitrag architekturunabhängiger generischer Systemdefinition**
	Konsequenzen-analyse	Die Konsequenzen einer Gefährdung können in Form von Wirkungszusammenhängen qualitativ beschrieben werden. Eine Quantifizierung der Konsequenzen ist nicht möglich, da quantifizierende Angaben wie z.B. die Einsatzbedingungen des Systems bei generischer Betrachtung nicht bekannt sind.
	Risikoabschätzung	Die Abschätzung oder Ermittlung des Risikos setzt die Kenntnis quantifizierender Faktoren wie das Schadensausmaß und die Übergangswahrscheinlichkeit von der Gefährdung zu einem Unfall voraus. Diese Werte können in Abhängigkeit von den Betriebsbedingungen unterschiedlich ausfallen. Es ist, wie z.B. der Unterschied zwischen einer Hochgeschwindigkeitsbahn und einer Bahn mit vereinfachten Betriebsverhältnissen nahelegt, offensichtlich, dass eine Quantifizierung stets eine Konkretisierung der Randbedingungen erfordert und damit nicht als generisch für alle Bahnen angesehen werden kann. Eine Risikoabschätzung kann nicht generisch für alle spurgeführten Verkehrssysteme sein. → nicht generisch durchführbar
	THR-Zuordnung	Sie setzt eine Risikoabschätzung voraus → nicht generisch durchführbar
„Mitte“	*H [Hazard = Gefährdung]*	s. Gefährdungsidentifikation
	THR	s. THR-Zuordnung
	Mögliche neue Gefährdungen	Sie sind nach der Norm mögliche Folgen bestimmter Funktionsrealisierungen, d.h. es handelt sich um realisierungsspezifische Ursachen für das Versagen betrieblicher Funktionen → für die generische Betrachtung ohne Bedeutung
Gefährdungsbeherrschung („unteres Dreieck“)	*Ursachenanalyse*	Die Gefährdungen müssen durch die gewählten Funktionsrealisierungen beherrscht werden. Eine Funktionsrealisierung ist eine von mehreren möglichen Realisierungen. Das „untere Dreieck“ kann nicht allgemeingültig sein. → nicht generisch durchführbar
	Common Cause-Analyse	
	SIL-Zuordnung	

4.1.4 Bezug zu Einzelfallbetrachtungen

Wie im Abschnitt 4.1.3 gezeigt worden ist, erlaubt eine architekturunabhängige generische Systemdefinition noch keine Risikobewertung. Eine solche Bewertung kann erst im Rahmen eines konkreten Vorhabens durchgeführt werden. Dazu müssen die entsprechenden Angaben bereitgestellt und mit der architekturunabhängigen generischen Systemdefinition zusammengefügt werden. Wenn dies geschehen ist, ist das Vorgehen im Sinne der CSM-Recommendation vollständig. Die architekturunabhängige generische Systemdefinition bildet den generischen Kern, der bei der Betrachtung konkreter Vorhaben um die entsprechenden Systemspezifika ergänzt werden muss, um z. B. Gefährdungsraten zu ermitteln (Bild 30).

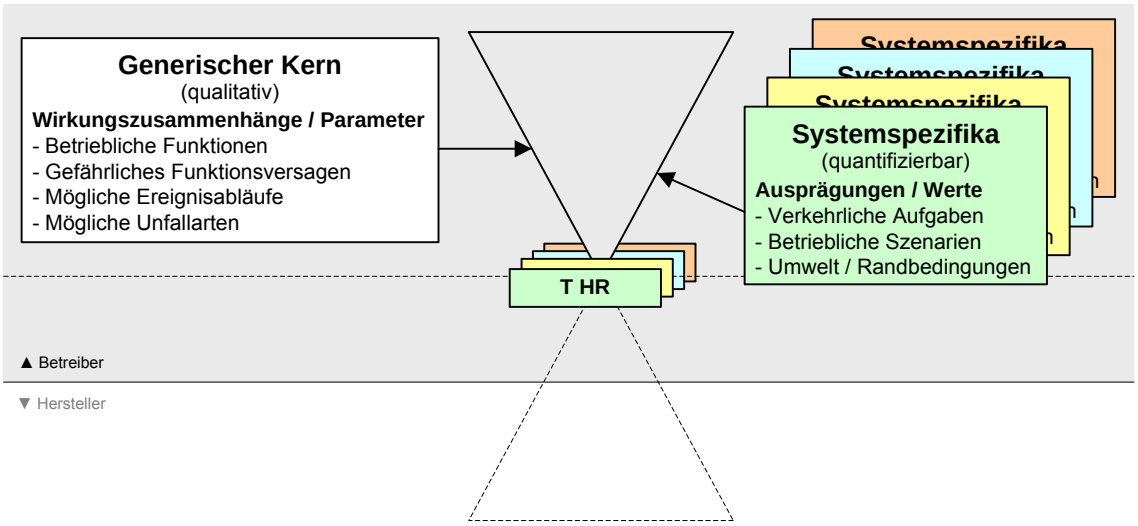


Bild 30: Zusammenfügen eines generischen Kerns mit den Spezifika von Einzelfällen

4.2 Formulierung generischer Funktionsdefinitionen

Mit der im Abschnitt 3 durchgeführten Analyse konnte gezeigt werden, dass im Eisenbahnwesen bislang überwiegend auf den Einzelfall bezogene Gefährdungslisten erstellt worden sind. Lediglich mit der prEN 15380-4 liegt eine Funktionsliste größeren Umfangs vor. Sie ist zwar für Fahrzeuge konzipiert worden, enthält aber mit den K-Funktionen einen Funktionsbereich, der den Betriebsverfahren zuzurechnen ist (vgl. Anhang 3). Die in der Vornorm

definierten Funktionen sind nach festgelegten Regeln formuliert worden[25] und enthalten neben einem einleitenden Verb die Angabe eines Objekts/einer Objektergänzung, bilden aber keine vollständigen Sätze. Trotz der Vorgaben wirken die Formulierungen z.T. schlagwortartig und lassen Interpretationsspielräume zu. Deshalb ist es aus dem Blickwinkel der Betriebsverfahren teilweise fraglich, ob es sich um zweckorientierte Funktionsformulierungen oder um Anforderungen zum Vorhalten bestimmter Formen von Funktionsträgern handelt. In der Kenntnis von Systemarchitekturen, aber auch aus dem eigentlichen Anwendungsgebiet Fahrzeuge heraus, mögen im Kreise von Fachleuten die Interpretationsspielräume eingeschränkt werden können. Soll aber, wie beim Definieren einer generischen Referenz für Betriebsverfahren angestrebt, auf entsprechende anfordernde Angaben verzichtet werden, müssen die Interpretationsspielräume weiter eingeschränkt und die Definitionen in funktionaler Hinsicht konkretisiert werden. Deshalb wird in diesem Abschnitt ein Vorgehen entwickelt, mit dem derartige Mängel durch einen systematischen grammatikalischen Aufbau der Funktionsformulierung vermieden werden können.

4.2.1 Anforderungen einschlägiger Normen

Die zu schaffenden Regeln zum Formulieren von Funktionsdefinitionen sollen sich an Definitionen des Begriffs „Funktion“ orientieren, die im Anwendungsgebiet gebräuchlich sind. Im Eisenbahnwesen darf dies für die in den Normen IEC 61226 und EN 50129 enthaltenen Definitionen angenommen werden. In der IEC 61226 wird Funktion als *„specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it”*[26] definiert. Die EN 50129 definiert Funktion als *„Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt“*.

Beiden Definitionen ist der Bezug zu dem Zweck bzw. zu dem Ziel gemeinsam, der bzw. das mit einer Funktion erreicht werden soll. Ebenfalls gemeinsam ist die Andeutung eines nicht näher benannten Funktionsträgers. In der IEC 61226 erfolgt dies indirekt mit dem Hinweis

[25] In der prEN 15380-4:2009 im Annex G gegebene Regeln zum Formulieren von Funktionen:

„For creation of function terms the following rules apply:

Rule 1: Each function shall consist of at least one verb in its verbal form and an object complement.

Rule2: The verb is defined in a dictionary. Preferred verbs are: to provide, to enable, to ensure, to command, to access.

Rule 3: The function name shall start with the verb.

Rule 4: Negative definition shall be avoided.

Rule 5: The function name shall be unambiguous.

Rule 6: Function names shall have an unambiguous abbreviation unless it is unavoidable.”

[26] Deutsche Übersetzung in [BEP08, S. 46] als „bestimmter Zweck oder zu erreichendes Ziel, das spezifiziert oder näher beschrieben werden kann, ohne Bezug auf die physikalischen Mittel zu nehmen“.

auf nicht näher zu spezifizierende „physikalische Mittel“; die EN 50129 verwendet den konkreter klingenden Begriff „Produkt“. Die Ausführung einer Funktion findet in der EN 50129 als „Art von Aktion oder Tätigkeit“ ihren Ausdruck. Diesen konkreten Bezug zu „Produkt“ enthält die IEC 61226 nicht; sie verweist auf eine Spezifizierung oder nähere Beschreibung des Zwecks oder Ziels, die keinen Bezug zu den physikalischen Mitteln haben soll. Als eine solche Spezifizierung des Ziels könnte die Art der in der EN 50129 genannten Aktionen oder Tätigkeiten aufgefasst werden, da diese das Erreichen des Zwecks bzw. des Ziels spezifiziert. Trotz dieser leicht unterschiedlichen Schwerpunktsetzungen sind beide Definitionen zueinander widerspruchsfrei. Sie lassen sich grundsätzlich in Übereinstimmung bringen und es können mit den Gliedern „Ziel / Zweck“, „Aktion / Tätigkeit“ und „Funktionsträger“ drei Elemente gegeneinander abgegrenzt werden, die zur Definition von Funktionen herangezogen werden können (Bild 31). [27]

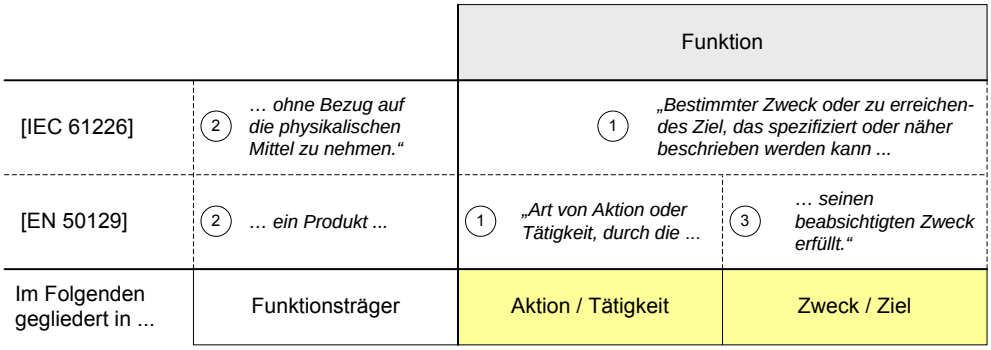


Bild 31: Elemente für das Definieren von Funktionen

4.2.2 Anforderungen an das Definieren generischer Funktionen

Für Funktionen, die generisch definiert werden sollen, dürfen sich aus der Funktionsdefinition keine Rückschlüsse auf die Realisierung des Funktionsträgers ergeben: Weder darf der Funktionsträger benannt werden, noch sollte er indirekt durch die Angabe der Aktion oder Tätigkeit angedeutet werden. Damit lassen sich für das Definieren generischer Funktionen folgende Anforderungen formulieren:

- Der mit der Funktion beabsichtigte Zweck oder das zu erreichende Ziel muss formuliert werden. (A1)

[27] Im Anwendungsgebiet wird der Begriff „Funktion“ auch für menschliche Funktionsträger verwendet. In [BRA10] wird beispielsweise von der Funktion Triebfahrzeugführer und der Funktion Fahrdienstleiter gesprochen. Die Verwendung des Begriffs Funktion in diesem Sinne ist umgangssprachlicher Natur und wird im Sinne von „Rolle“ verstanden: „In Ihrer Funktion als …“ ist synonym zu „In Ihrer Rolle als …“.

- Um den Zweck / das Ziel eindeutig formulieren zu können, kann zur Abgrenzung eine Aktion / Tätigkeit angegeben werden, mit der der Zweck / das Ziel erreicht werden soll. (A2)
- Die Formulierung einer Aktion oder der Tätigkeit muss funktionsträgerneutral sein. (A3)
- Die Angabe eines bestimmten Funktionsträgers oder seiner Art ist unzulässig. (A4)

Beispiel „Herstellung von Mehl“

Am Beispiel der Herstellung von Mehl werden in der Tabelle 13 verschiedene Funktionsformulierungen dahingehend bewertet, inwieweit sie die Anforderungen (A1) bis (A4) erfüllen. Die beispielhaften Funktionsformulierungen orientieren sich z.T. auch an Formulierungen, wie sie bei der Analyse der prEN 15380-4 im Abschnitt 3.2.3 vorgefunden worden sind.

Tabelle 13: Beurteilung unterschiedlicher Arten von Funktionsformulierungen

		A1	A2	A3	A4	Erläuterung
a)	Mühle vorhalten	f	f	f	f	(A1) f: Es wird kein Zweck / kein Ziel beschrieben. (A2, A3) f: Es wir keine Aktion / keine Tätigkeit angedeutet. Das „Vorhalten“ einer Mühle ist keine Aktion oder Tätigkeit, die ein Produkt (Mehl) o.ä. erzeugt. (A4) f: Es wird ein konkreter Funktionsträger genannt.
b)	Getreide mahlen	f	(ok)	(f)	ok	(A1) f: Es wird kein Zweck / kein Ziel beschrieben. (A2) (ok): Die Aktion / die Tätigkeit wird beschrieben. (A3) (f) „mahlen“ könnte aber als Hinweis auf die Realisierungsart verstanden werden. (A4) ok: Der Funktionsträger wird nicht genannt.
c)	Mahlen von Getreide ermöglichen	f	f	f	ok	(A1) f: Es wird kein Zweck / kein Ziel beschrieben. (A2, A3) f: Durch „Mahlen ermöglichen„ wird die Aktion / die Tätigkeit nur indirekt beschrieben; „mahlen“ könnte ferner als Hinweis auf die Realisierungsart verstanden werden. (A4) ok: Der Funktionsträger wird nicht genannt.
d)	Mehl herstellen	ok	(f)	ok	ok	(A1) ok: Der Zweck / das Ziel wird beschrieben. (A2) (f): Es wird eine Aktion / eine Tätigkeit angedeutet, die ein Ziel erkennen lässt. Sie könnte jedoch näher spezifiziert werden, ohne dass dadurch Bezüge zu dem physikalischen Mittel entstehen. (A3) ok: Das Verb „herstellen“ ist funktionsträgerneutral. (A4) ok: Der Funktionsträger wird nicht genannt.

		A1	A2	A3	A4	Erläuterung
e)	Getreide zu Mehl mahlen	ok	ok	(f)	ok	(A1) ok: Der Zweck / das Ziel wird beschrieben. (A2) ok: Es wird eine Aktion / Tätigkeit angegeben. (A3) (f): Durch das Verb „mahlen“ kann als Lösung eine Mühle suggeriert werden; es ist nicht funktionsträgerneutral, denn das Getreide könnte jedoch z.B. auch mit Mörser und Stößel zu Mehl verarbeitet werden. (A4) ok: Der Funktionsträger wird nicht genannt.
f)	Getreide zu Mehl verarbeiten	ok	ok	ok	ok	(A1) ok: Der Zweck / das Ziel wird beschrieben. (A2) ok: Durch das Verb wird eine Aktion / eine Tätigkeit angedeutet, die auf eine zum Ziel führende Veränderung hindeutet. (A3) ok: Das Verb ist neutral, es suggeriert keinen Funktionsträger. (A4) ok: Der Funktionsträger wird nicht genannt.
g)	Der Funktionsträger verarbeitet Getreide zu Mehl.	Ok	ok	ok	ok	(A1) ok: Der Zweck / das Ziel wird beschrieben. (A2) ok: Durch das Verb wird eine Aktion / eine Tätigkeit angedeutet, die auf eine zum Ziel führende Veränderung des Objekts hindeutet. (A3) ok: Das Verb ist neutral, es suggeriert keinen Funktionsträger. (A4) ok: Durch den neutralen Begriff „Funktionsträger“ wird das Vorhandensein eines physikalischen Mittels angedeutet, aber nicht genannt; seine Verwendung erlaubt die Formulierung der Funktion als ganzen Satz.

Insbesondere die Formulierungen e), f) und g) erlauben gute Vorstellungen von der zu definierenden Funktion. Für alle anderen Funktionsformulierungen wird aufgrund der unvollständigen Formulierungen entsprechendes Hintergrundwissen über die beabsichtigte Aktion oder Tätigkeit benötigt. Damit geht die Gefahr einer unterschwelligen Betrachtung bestimmter Funktionsrealisierungen einher. Diese muss beim Definieren generischer Funktionen vermieden werden. Mit den Formulierungen f) und g) gelingt das gut. Mit dem im Sinne eines Platzhalters genutzten Begriff „Funktionsträger“ kann zudem der Anspruch unterstrichen werden, die Funktion generisch definieren zu wollen.

Die Formulierung der Funktion wie in g) als ganzer Satz erleichtert die Benennung einer Aktion / einer Handlung und eines Ziels / eines Zwecks der Funktion. Dies hilft missverständliche oder ungenaue Formulierungen wie jene unter a) bis e) zu vermeiden.

4.2.3 Verwendung von Satzgliedern

In dem vorhergehenden Abschnitt sind am Beispiel „Herstellung von Mehl“ Funktionen z.T. als vollständige Sätze formuliert worden. Deren grammatikalische Strukturen können auch auf die Elemente einer Funktionsdefinition bezogen werden: Die Satzglieder Prädikat und Objekt sowie die Angabe einer adverbialen Bestimmung des Zwecks sind deckungsgleich mit den Funktionselementen „Aktion / Tätigkeit“ und „Zweck / Ziel“ (Bild 32). Sie bieten die Möglichkeit, das Formulieren von Funktionsdefinitionen durch die Vorgabe einer einheitlichen Satzbaustruktur zu unterstützen und auf diese Weise insgesamt homogenere Funktionsformulierungen zu erhalten.

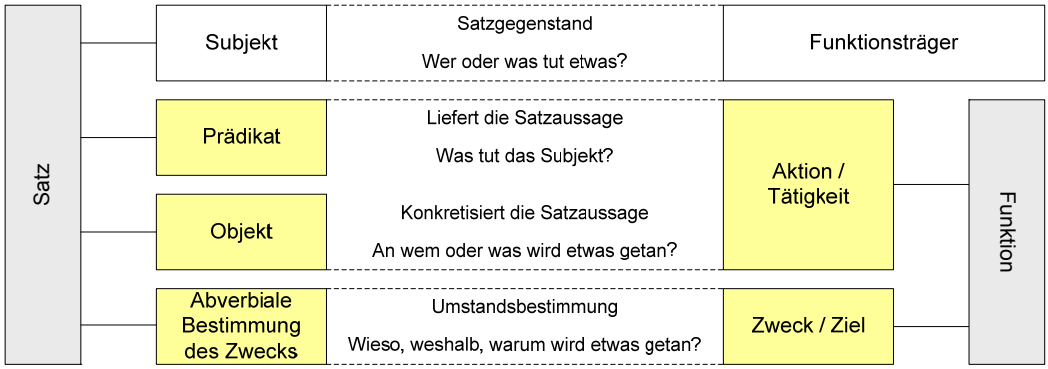


Bild 32: Bezug zwischen Satzbau und Funktionsdefinition

Die Aktion oder Tätigkeit wird durch das Prädikat und eine ergänzende Angabe eines oder mehrerer Objekte ausgedrückt. Das Prädikat liefert die grundsätzliche Satzaussage und kann durch das Hinzufügen eines oder mehrerer Objekte konkretisiert werden. Deshalb ist ein Satz, wie z.B. „Der Funktionsträger stellt die Weiche“, auch ohne adverbiale Zweckbestimmung grammatikalisch vollständig. Aus funktionaler Sicht ist er jedoch unvollständig, da eine Zweckbestimmung fehlt. Der Zweck würde sich in diesem Fall nur durch Fachkenntnis erschließen. Eine als Satz formulierte Funktionsdefinition muss folglich eine adverbiale Bestimmung enthalten, mit der der Zweck der Aktion oder der Tätigkeit ausgedrückt wird. Anhand der folgenden drei Beispiele werden jeweils mehrere Möglichkeiten der Formulierung erörtert.

Beispiel 1:

<table>
<tr><td>Der Funktionsträger</td><td>stellt</td><td>die zu befahrende Weiche</td><td>in die von der Fahrt benötigte Endlage.</td></tr>
<tr><td rowspan="2">Subjekt (generisch)</td><td>Prädikat</td><td>Objekt</td><td>Adverbiale Bestimmung des Zwecks</td></tr>
<tr><td colspan="2">Aktion / Tätigkeit</td><td>Zweck / Ziel</td></tr>
</table>

„Der Funktionsträger stellt die zu befahrende Weiche“ ist bereits ein vollständiger Satz. Der mit dieser Aktion oder Tätigkeit verfolgte Zweck ergibt sich durch den Zusatz „in die von der Fahrt benötigte Endlage“. Das Prädikat und die adverbiale Bestimmung des Zwecks können

gut voneinander unterschieden werden. Alternativ kann der Zweck aber auch als Nebensatz mit „um … zu“, einen Finalsatz, formuliert werden:

Der Funktionsträger	stellt	die zu befahrende Weiche,	um sie [die Weiche] in die von der Fahrt benötigte Endlage zu bringen.
Subjekt (generisch)	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
	Aktion / Tätigkeit		*Zweck / Ziel*

Mit der Formulierung als Finalsatz wird prägnanter zwischen der Aktion oder Tätigkeit und dem damit verfolgten Zweck unterschieden. Es wird zudem hervorgehoben, dass der verfolgte Zweck ein Ergebnis der Aktion oder Tätigkeit ist.

Soll im Hinblick auf eine generische Formulierung nicht nur das Subjekt, sondern auch die Aktion oder Tätigkeit neutral ausgedrückt werden, kann dies nur unter Verwendung des Finalsatzes geschehen. Mit dem Finalsatz wird gewährleistet, dass die Funktion trotz der dann stereotypischen SPO-Formulierungen (Subjekt, Prädikat, Objekt), wie z.B. „Der Funktionsträger“ und „führt eine Aktion / Tätigkeit aus“, ohne einen inhaltlichen Verlust bzgl. Des Funktionszwecks definiert werden kann:

Der Funktionsträger	führt eine Aktion / Tätigkeit aus,		um die Weiche in die von der Fahrt benötigte Endlage zu bringen.
Subjekt	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
Generische SPO-Formulierung			*Zweck / Ziel*

Aus dieser Formulierung kann, sofern gewünscht, eine stichwortartige generische Funktionsdefinition abgeleitet werden: „Weiche in die von der Fahrt benötigte Endlage bringen“.

Der so schriftlich fixierte Informationsgehalt ist im Gegensatz zu „*control switches*“ [BEP08, S. 205] nicht tätigkeits-, sondern zweck- und ergebnisorientiert. Die möglichen Ergebnisse lassen sich unter Wahrung sprachlicher Bezüge unmittelbar aus der Formulierung ableiten: a) „benötigte Endlage“ bei erfolgreicher Ausführung sowie b) „andere Endlage“ und c) „keine Endlage“ bei erfolgloser Ausführung. Die Möglichkeiten einer unmittelbaren Verknüpfung der generischen Funktionsdefinition mit der Gefährdungsidentifikation werden deutlich (vgl. a. 4.3.3).

Beispiel 2:

Der Funktionsträger	prüft	den zu befahrenden Gleisabschnitt	auf die Belegung durch andere Fahrten oder Fahrzeuge.
Subjekt (generisch)	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
	Aktion / Tätigkeit		*Zweck / Ziel*

Auch in diesem Beispiel ist der aus Subjekt, Prädikat und Objekt gebildete Satz „Der Funktionsträger prüft den zu befahrenden Gleisabschnitt“ grammatikalisch vollständig. Er bedarf aber, um den Anforderungen an eine Funktionsdefinition zu genügen, ebenfalls einer adverbialen Bestimmung des Zwecks. Dies ist auch deshalb geboten, da sich die ausgedrückte Aktion oder Tätigkeit, auch auf andere Aspekte, wie z.B. den baulichen Zustand des Gleises, beziehen könnte. Die Adverbiale Bestimmung des Zwecks wird in diesem Beispiel als „auf das Freisein von anderen Fahrzeugen“ formuliert. Alternativ kann auch in diesem Fall ein Finalsatz gebildet werden:

Der Funktionsträger	prüft	den zu befahrenden Gleisabschnitt,	um die Belegung [des Gleises] durch andere Fahrzeuge zu ermitteln.
Subjekt (generisch)	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
	Aktion / Tätigkeit		*Zweck / Ziel*

Ähnlich dem Beispiel 1 wird durch die Formulierung eines Finalsatzes auch in diesem Fall die Unterscheidung zwischen der Aktion oder Tätigkeit und dem damit verfolgten Zweck deutlicher hervorgehoben.

In diesem Fall kann die Funktion ohne inhaltlichen Verlust bzgl. des Funktionszwecks als generische SPO-Formulierung ausgedrückt werden:

Der Funktionsträger	führt eine Aktion / Tätigkeit aus,		um die Belegung des zu befahrenden Gleises durch andere Fahrzeuge zu ermitteln.
Subjekt	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
Generische SPO-Formulierung			*Zweck / Ziel*

Auch aus dieser Formulierung kann eine stichwortartige generische Formulierung mit einem zweck- und ergebnisorientierten Inhalt abgeleitet werden: „Ermittlung der Belegung des zu befahrenden Gleises durch andere Fahrzeuge“.

Die möglichen Ergebnisse lassen sich unter Wahrung sprachlicher Bezüge unmittelbar aus der Formulierung ableiten: a) „belegt von anderen Fahrzeugen“ und b) „frei von anderen Fahrzeugen“ und c) „keine Information“ bei erfolgloser Ausführung. Auch hier sind die Möglichkeiten einer unmittelbaren Verknüpfung der generischen Funktionsdefinition mit der Gefährdungsidentifikation gegeben (vgl.a. 4.3.3).

Beispiel 3:

Der Funktionsträger	ermittelt	die zwischen Start und Ziel liegenden Fahrwegelemente.	
Subjekt (generisch)	*Prädikat*	*Objekt*	*Adverbiale Bestimmung des Zwecks*
	Aktion / Tätigkeit		*Zweck / Ziel*

Dieses Beispiel scheint auf den ersten Blick als Funktionsdefinition vollständig zu sein, da sich aus fachkundiger Sicht der Zweck der Funktion zu erschließen scheint. Formuliert man jedoch „Der Funktionsträger ermittelt Fahrwegelemente“, wird deutlich, dass es sich bei der dann erforderlichen Ergänzung „die zwischen Start und Ziel liegen“ um einen Relativsatz, nicht aber um einen Finalsatz handelt; die für einen Finalsatz typische Frage „Warum werden die Fahrwegelemente ermittelt?“ bleibt unbeantwortet. Die Verwendung eines Finalsatzes mit „um .. zu“ erzwingt auch hier die Angabe des Zwecks:

Der Funktionsträger	ermittelt	Fahrwegelemente,	um bei der Bereitstellung des Fahrwegs alle zwischen Start und Ziel benötigten [Fahrwegelemente] zu berücksichtigen.
Subjekt (generisch)	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
	Aktion / Tätigkeit		*Betrieblicher Zweck*

Die Aktion oder Tätigkeit kann ohne inhaltlichen Verlust bzgl. Des Funktionszwecks generisch ausgedrückt werden:

Der Funktionsträger	führt eine Aktion / Tätigkeit aus,		um bei der Bereitstellung des Fahrwegs alle zwischen Start und Ziel benötigten Fahrwegelemente zu berücksichtigen.
Subjekt	*Prädikat*	*Objekt*	*Adverbiale Best. d. Zwecks als Finalsatz*
Generische SPO-Formulierung			*Zweck / Ziel*

Auch aus dieser Formulierung kann eine stichwortartige generische Formulierung mit einem zweck- und ergebnisorientierten Inhalt abgeleitet werden: „Berücksichtigung aller zwischen Start und Ziel benötigten Fahrwegelemente bei der Bereitstellung des Fahrwegs“. Aber auch bei ihr kann nicht mehr so eindeutig zwischen Zweckbestimmung und Ausführung unterschieden werden, wie bei der Formulierung mit „um … zu“.

Für den Fall der erfolgreichen Funktionsausführung kann als Ergebnis „Liste der zwischen Start und Ziel benötigten Fahrwegelemente“ abgeleitet werden. Für die nicht erfolgreiche Funktionsausführung lassen sich die Ergebnisse „keine Liste …“ oder „unvollständige Liste …“ angeben.

Erkenntnisse

Die Erörterung der vorstehenden Formulierungsbeispiele führt im Hinblick auf eine mögliche Verwendung grammatikalischer Satzbaustrukturen zu folgenden Erkenntnissen:

- Funktionen können grundsätzlich auch unter Verwendung der Satzglieder „Subjekt“, „Prädikat“, „Objekt“ und „Adverbiale Bestimmung des Zwecks“ als vollständiger Satz

formuliert werden; sollen in generische Formulierungen ein Subjekt und ein Prädikat einbezogen werden, sind diese realisierungsunabhängig zu formulieren.

- Die Bestimmung des Zwecks ist die zentrale inhaltliche Aussage einer Funktionsdefinition; sie ist unverzichtbar für jede Funktionsdefinition.
- Der Zweck ist das Ergebnis einer Aktion oder Tätigkeit; er lässt sich unabhängig von der Aktion oder Tätigkeit und damit auch unabhängig von einem Funktionsträger definieren.
- Funktionen können deshalb nicht nur ohne konkrete Angaben zum Funktionsträger, sondern auch ohne Konkretisierung der Art der Aktion oder Tätigkeit definiert werden; mit der Angabe einer Aktion oder Tätigkeit wird der Zweck jedoch deutlicher als das damit hervorgerufene Ergebnis dargestellt.
- Die Formulierung der adverbialen Bestimmung des Zwecks als Finalsatz mit „um … zu“ erlaubt eine eindeutige Unterscheidung zwischen der Aktion oder Tätigkeit und dem damit zu erreichenden Zweck oder Ziel.
- Im Hinblick auf die Gefährdungsidentifikation ist die Unterscheidung zwischen Zweckbestimmung und Ausführung von Interesse, da zwischen Funktionsausführung und Ergebnis ein Ursache-Wirkungsverhältnis besteht, das für die Identifikation generischer Gefährdungen herangezogen werden kann (vgl. a. 4.3.3).

Das Definieren von Funktionen in Form vollständiger Sätze kann die inhaltliche Präzisierung unterstützen. Es trägt insbesondere zur Herausarbeitung des Unterschiedes zwischen der Zweckbestimmung und der Funktionsausführung bei. Auch beim Definieren generischer Funktionen, bei denen die Funktionsausführung ebenso wie der Funktionsträger in den Hintergrund treten muss, kann die Definition der Zweckbestimmung durch die Formulierung eines vollständigen Satzes mit Finalsatz unterstützt werden. Dies schließt jedoch nicht aus, sich bei der Wahl eines ergänzenden „griffigen“ Funktionsnamens einer als generisch anzusehen Aktion oder Tätigkeit zu bedienen.

4.2.4 Inhalt einer Funktionsdefinition

Die vorstehenden Ausführungen decken sich mit der in der IEC 61226 enthaltenen Definition des Begriffs Funktion, die allein auf den Zweck und nicht wie die EN 50129 mehr auf die Aktion bzw. Tätigkeit fokussiert. Deshalb sollte in Anlehnung an die IEC 61226, aber ohne im Widerspruch zur EN 50129 zu stehen, eine Funktionsdefinition folgenden Anforderungen entsprechen:

In einer (generischen) Funktionsdefinition ist ein bestimmter Zweck bzw. ein bestimmtes Ziel zu beschreiben, der bzw. das im Sinne eines Ergebnisses mit einer von einem Funktionsträger ausgeführten Aktion oder Tätigkeit erreicht werden soll.

Angaben zur Aktion oder Tätigkeit und zum Funktionsträger sind optional.

Bei generischen Funktionsdefinitionen sind konkretisierende Angaben zur Aktion oder Tätigkeit sowie zum Funktionsträger nicht zulässig. Diese Anforderung kann durch realisierungsunabhängige Formulierungen bzw. den Verzicht auf entsprechende Angaben erfüllt werden.

Die Ausführungen der Abschnitte 4.2.1 bis 4.2.3 werden abschließend in Tabelle 14 zusammengefasst und erläutert.

Tabelle 14: Elemente einer generischen Funktionsdefinition

Zweck-bestimmung	„muss enthalten sein“	Mit dem Zweckbestimmungselement wird der Zweck oder das Ziel beschrieben, denen die Funktion dienen soll; es wird keine Aktion oder Tätigkeit beschrieben, mit der die Funktion ausgeführt wird. Die Zweckbestimmung wird als adverbiale Bestimmung des Zwecks formuliert; ihre Formulierung als Finalsatz mit „um … zu“ unterstützt die Abgrenzung des Zweckbestimmungselements gegenüber der Aktion / Tätigkeit. In der adverbialen Bestimmung ggf. enthaltene Verben sind nicht gleichbedeutend mit einer Aktion / Tätigkeit. Sie drücken keine Aktion oder Tätigkeit des Funktionsträgers aus. Die Zweckbestimmung bildet den Ausgangspunkt für die Identifizierung betrieblicher Gefährdungen (vgl. Abschnitt 4.3.3).
Aktion / Tätigkeit	„darf enthalten sein“	Mit der Aktion / Tätigkeit kann eine prinzipielle Arbeitsweise der Funktion beschrieben werden, mit der der Zweck oder das Ziel der Funktion erreicht werden soll; dies kann das Verständnis erleichtern. Bei generischen Funktionsdefinitionen sollte ein möglichst realisierungsneutrales Prädikat gewählt werden, wie z.B. „führt eine Aktion / Tätigkeit aus, …“.
Subjekt	„darf enthalten sein“	Ein Subjekt kann ergänzend angegeben werden; seine Verwendung erlaubt das Formulieren aktiver Funktionsdefinitionen, d.h. das Objekt wird nicht „behandelt“, sondern das Subjekt „behandelt“ das Objekt. Bei schon vorliegenden Realisierungsvorstellungen kann der Funktionsträger konkret benannt werden; bei generischen Definitionen kann als Subjekt z.B. die realisierungsneutrale Formulierung „Der Funktionsträger“ verwendet werden.

4.3 Identifizierung generischer Gefährdungen

Neben der Definition von Funktionen ist die Identifizierung der bei einem Versagen der Funktionen möglicherweise eintretenden Gefährdungen ein weiterer wichtiger Bestandteil des Sicherheitsanalyseprozesses. Eine Gefährdungsidentifikation kann sowohl auf Basis konkreter Systementwicklungen als auch auf der Basis definierter Funktionen durchgeführt werden. Die dafür notwendige Ermittlung der Ausfallarten eines Systems erfolgt i.d.R. mit Analysenmethoden, die durch ein strukturiertes Vorgehen geprägt sind. Im Folgenden wird mit der Failure Mode and Effects Analysis (FMEA) ein im Anwendungsgebiet bei der Entwicklung von Systemen verbreitetes und erprobtes Vorgehen vorgestellt (4.3.1), das seinem ursprünglichen Zweck entsprechend i.d.R. auf Komponentenebene arbeitet. Im Abschnitt 4.3.2 wird auf die Anwendung dieser Methode auf generisch definierte Funktionen eingegangen und auf Basis der dabei gemachten Erfahrungen in den Abschnitten 4.3.3 ff das Vorgehen bei der Identifizierung von Gefährdungen modifiziert.

4.3.1 Failure Mode and Effects Analysis

Die Failure Mode and Effects Analysis (FMEA) ist eine Methode zur Analyse der Ausfallarten eines Systems und der aus den Ausfällen resultierenden Auswirkungen. Mit der FMEA werden zuverlässigkeits-, sicherheits- und instandhaltungsrelevante Informationen über ein System systematisch erfasst und bewertet, um Schwachstellen innerhalb des Systems zu identifizieren und Maßnahmen zur Risikominimierung ableiten zu können. Im Einzelnen soll eine FMEA nach [EN 60812, S. 8] folgenden Zielen dienen:

- Identifizierung und Beurteilung der Auswirkungen eines Ausfalls im Gesamtsystem, vor allem solcher Ausfälle, die unerwünschte Auswirkungen auf den Systembetrieb haben;
- Identifizierung kritischer Komponenten, um Gefahren und Risiken zu minimieren und um die Instandhaltung optimal zu planen;
- Aufdeckung der Schwachstellen eines Prozesses, um den Prozess zu optimieren;
- Bereitstellung von Hilfen für die Fehlzustandsdiagnose;
- Klassifizierung der erkannten Ausfallarten entsprechend relevanter Eigenschaften, wie z.B. Erkennbarkeit, Diagnosefähigkeit, Prüfbarkeit, Austauschbarkeit von Einheiten, Vorkehrungen für Ersatz und Betrieb;
- Beseitigung von Fehlerursachen (Korrekturmaßnahmen) und Verbesserung der Systemfunktionsfähigkeit.

Eine FMEA wird i.d.R. formalisiert durchgeführt, um im Hinblick auf ein möglichst vollständiges Ergebnis ein systematisches Vorgehen zu gewährleisten. Sie beginnt mit einer umfassenden Definition des technischen Systems, die in Abhängigkeit von der Art des Systems i.d.R. folgende Punkte umfasst:

- Definition des Systems und seiner Funktionen,

- Beschreibung der Schnittstellen und Wechselwirkungen mit anderen Systemen,
- Festlegung der Systemkomponenten und –zustände,
- Angabe der Umgebungsbedingungen und der Betriebsbelastungen,
- Vorgabe von Zuverlässigkeitsanforderungen.

Betrachtungseinheiten sind i.d.R. die Systemkomponenten. Ausgehend von den Fehlzuständen der Betrachtungseinheiten werden die möglichen Auswirkungen im System analysiert. In die Analyse fließen Einflussfaktoren wie z.B. die festgelegten Betriebsparameter und Umgebungsbedingungen ein. Für jede Betrachtungseinheit werden die jeweils denkbaren Ausfallarten und –ursachen ermittelt und deren Auswirkungen auf die jeweils übergeordneten Betrachtungseinheiten beschrieben. Dies geschieht i.d.R. tabellarisch. Die Ausfallarten lassen sich im Allgemeinen aus den Funktionen einer Betrachtungseinheit und die Auswirkungen aus weiteren Systeminformationen ableiten. Wesentlich für den Aussagewert der Analyse ist, dass möglichst alle Ausfallarten einer Betrachtungseinheit bestimmt werden. Dazu können als Anhaltspunkte Schlüsselworte verwendet werden, die ein systematisches Auffinden der Ausfallarten unterstützen. Typische Schlüsselworte zum Identifizieren der Ausfallarten sind zum Beispiel: „geht nicht“, „ungewollt / falsch“, „zur Unzeit (zu früh / zu spät)“, „zu niedrig / zu hoch“ und „zu wenig / zu viel“, die gut auf die von einer Betrachtungseinheit ausgeführte Aktion oder Tätigkeit angewendet werden können. Die Schlüsselworte entstammen dem Bereich elektrotechnischer Bauteile, einem der ursprünglichen Einsatzbereiche der FMEA.

4.3.2 Anwendung der FMEA auf generisch definierte Funktionen

Die in [EN 60812] gegebene Beschreibung der FMEA geht vom Vorliegen relativ konkreter Vorstellungen über eine Systemrealisierung aus. Die im Fokus dieser Arbeit stehenden betrieblichen Funktionen müssen jedoch realisierungsunabhängig definiert werden. Daher können und dürfen im Rahmen der Gefährdungsidentifikation keine Bezüge auf Systemkomponenten genommen werden. Auch die Angabe von Aktionen oder Tätigkeiten ist nur begrenzt möglich, wenn die Anforderung an eine generische Formulierung nicht verletzt werden soll. Dies schließt die Anwendung der FMEA auf generisch definierte Funktionen nicht aus, es liegen jedoch andere Randbedingungen vor.

Erfahrungen

Funktionen, die generisch, d. h. nur durch den Zweck, definiert worden sind, weisen einen geringeren Konkretisierungsgrad auf als jene, für die bereits ein Funktionsträger und/oder Angaben zur Aktion oder Tätigkeit näher spezifiziert worden sind. Eine unmittelbare Anwendung der mehr aktions- oder tätigkeitsorientierten Schlüsselworte auf die bezweckten Funktionsziele kann deshalb zu FMEA-Ergebnissen führen, die größere Interpretationsspielräume zulassen. Um diese Spielräume einzuschränken, besteht die Möglichkeit, die Schlüsselworte vorab zu „interpretieren“. Tabelle 15 enthält Beispiele für die Vorab-

Interpretation der Schlüsselworte, wie sie in Eisenbahn- und Magnetschwebebahn-Projekten verwendet worden sind, an denen der Autor mitgewirkt hat.

Tabelle 15: Beispiele für die Vorab-Interpretation der FMEA-Schlüsselworte

Schlüsselwort	Verwendung im Sinne von
geht nicht	Die Funktion arbeitet nicht und liefert keine Informationen/Werte.
Ungewollt / falsch	Die Funktion liefert falsche Informationen/Werte.
Zur Unzeit (zu früh / zu spät)	Bezogen auf die Fahrt beginnt oder endet die Funktion zu früh bzw. zu spät.
Zu niedrig / zu hoch	Die Funktion macht Fehler in der Einhaltung/Prüfung stetiger Größen wie z.B. Geschwindigkeit oder Spurweite.
Zu wenig / zu viel	Die Funktion macht Fehler in der Einhaltung/Prüfung diskreter Größen wie z.B. Anzahl von Elementen.

Aufgrund des systematischen, sich in seinen Schritten auch bei generischen Funktionen wiederholenden Vorgehens sind auch in diesen Projekten die FMEA in tabellarischer Form durchgeführt worden. Im Bild 33 ist beispielhaft der prinzipielle Aufbau solcher Tabellen dargestellt. Die Spalte „Checkliste“ enthält die Schlüsselworte, mit deren Hilfe in der Spalte „Versagensart“ die Funktionsversagen formuliert werden. In Abhängigkeit von der Art der Funktion kann i.d.R. nicht bei jedem Schlüsselwort eine inhaltlich sinnvolle und nachvollziehbare Versagensformulierung gefunden werden. Die entsprechenden Zeilen bleiben leer (in Bild 33 grau dargestellt). Für die identifizierten Versagensarten werden die jeweils folgenden Abläufe skizziert und deren mögliche Folgen angegeben. Kann die Folge ein Unfall sein, wird das entsprechende Funktionsversagen als „Gefährdung“ eingestuft (in Bild 33 rot markiert).

Funktion		Checkliste	Versagensart	Ablauf	Folge	Bemerkung
FWS-3.1	Bahnübergang sichern	geht nicht	Der Bahnübergang kann nicht gesichert werden.	Die Fahrt kann nicht stattfinden.	Betriebshemmnis	Gemeint ist: Der Ausfall wird offenbart!
		zur Unzeit (zu früh / zu spät)	Der Bahnübergang wird zu früh gesichert.	Der Bahnübergang wird zu lange gesichert.	Behinderung anderer Verkehrsteilnehmer	Bei zu langer Sicherung werden Wegebenutzer ungeduldig und könnten den Bahnübergang trotz Sicherung benutzen
			Die Sicherung des Bahnübergangs wird zu früh aufgehoben.	Fahrzeug befährt nicht gesicherten Bahnübergang.	**Zusammenprall**	
			Der Bahnübergang wird zu spät gesichert.			sofern unerkannt -> entspricht "ungewollt / falsch" falls rechtzeitig erkannt -> "geht nicht"
			Die Sicherung des Bahnübergangs wird zu spät aufgehoben.	Der Bahnübergang wird zu lange gesichert.	Behinderung anderer Verkehrsteilnehmer	
		ungewollt / falsch	Der Bahnübergang ist gesichert, obwohl keine Fahrt stattfinden soll.	Der Bahnübergang ist unnötig gesichert.	Behinderung anderer Verkehrsteilnehmer	
			Der Bahnübergang ist nicht gesichert.	Fahrzeug befährt nicht gesicherten Bahnübergang.	**Zusammenprall**	
		zu niedrig / zu hoch				
		zu wenig / zu viel				

Bild 33: Beispiel für eine tabellarisch aufgebaute FMEA

Kritik

Die Anwendbarkeit einer schlüsselwortbasierten FMEA auf generisch definierte Funktionen ist in praxisrelevanten Projekten bestätigt worden. Dennoch sind im Rahmen der FMEA-Durchführung Schwachpunkte aufgefallen. Die Vorab-Interpretation der Schlüsselworte (Tabelle 15) hat die Interpretationsspielräume nicht im erwünschten Maß reduziert. Die Versagens- und die Gefährdungsformulierungen haben deshalb im Kreise der beteiligten Fachleute mehrfach zu längeren Diskussionen geführt. Sie galten u.a. der Frage, ob zwischen den für eine Funktion formulierten Versagen Abhängigkeiten im Sinne von Ursache und Wirkung bestehen würden. In dem im Bild 33 wiedergegebenen FMEA-Auszug wird beispielsweise unter „Versagensart“ „Der Bahnübergang ist nicht gesichert“ als Gefährdung angegeben. Mit dieser Formulierung wird ein Zustand des Bahnübergangs beschrieben, der das Ergebnis eines nicht näher bestimmten Ausführungsversagens ist. Die Formulierung der anderen Gefährdung als „Die Sicherung des Bahnübergangs wird zu früh aufgehoben“ beschreibt dagegen eine fehlerhafte Ausführung einer Aktion oder Tätigkeit, in deren Folge das falsche Funktionsergebnis „Der Bahnübergang ist nicht gesichert“ stehen würde. Würde dagegen „Der Bahnübergang ist nicht gesichert“ als „Der Bahnübergang wird nicht gesichert“ formuliert, entspräche dies der Formulierung einer weiteren fehlerhaften Ausführung der Aktion oder Tätigkeit. Sie führt ihrerseits zu dem falschen Funktionsergebnis „Der Bahnübergang ist nicht gesichert“. Beide Aktionen oder Tätigkeiten sind fehlerhaft und ursächlich für das falsche Funktionsergebnis (Bild 34).

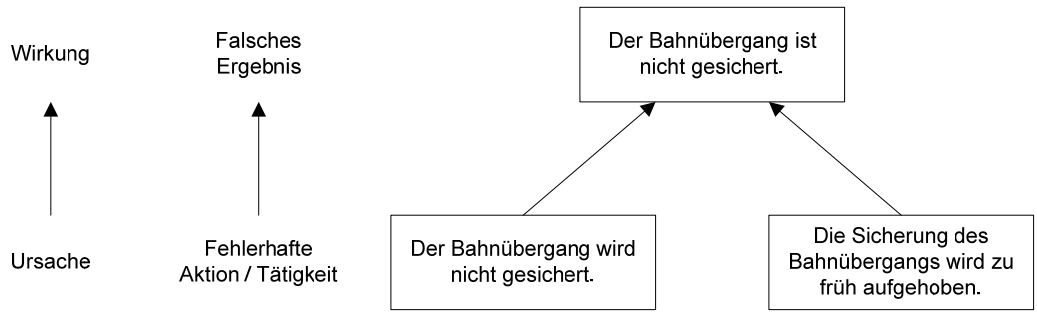


Bild 34: Ursache-Wirkung-Prinzip zwischen Aktion / Tätigkeit und Ergebnis

Fazit

Die Durchführung einer FMEA mit Schlüsselworten ist auch bei generisch definierten Funktionen möglich. Da sie nicht darauf ausgelegt ist, zwischen fehlerhaften Aktionen und Tätigkeiten einerseits und falschen Ergebnissen andererseits zu unterscheiden, kann es bei der Auflistung der identifizierten „Gefährdungen“ jedoch zu Verletzungen der Ursache-Wirkungszusammenhänge kommen und „gefährliche“ Ergebnisse auf derselben Ebene wie die sie verursachenden „gefährlichen“ Aktionen oder Tätigkeiten betrachtet werden. Da, wie am vorstehenden Beispiel deutlich wird, bereits kleinere Formulierungsunterschiede ausschlaggebend sein können, erfordert die Vorgehensweise mit Schlüsselworten eine besondere Sorgfalt. Deshalb sollte im Hinblick darauf, dass generische Funktionen ohnehin

nur durch die Angabe ihres Zwecks generisch definiert werden können, die Identifikation generischer Gefährdungen konsequenterweise allein auf der Zweckebene, d.h. auf der Ebene der durch die Funktionsausführung bewirkten Ergebnisse durchgeführt werden. Im Abschnitt 4.3.3 wird die FMEA für generisch definierte Funktionen dahingehend modifiziert, dass gefährliche Ergebnisse, die sie bewirkenden und deshalb gefährlichen Funktionsausführungen und die diese wiederum auslösenden Fehler und Ausfälle ihren Ebenen entsprechend getrennt identifiziert werden können.

4.3.3 Modifizierte Gefährdungsidentifikation

Das im Abschnitt 4.2 entwickelte Vorgehen, bei der Definition von Funktionen zwischen Zweckbestimmung und Funktionsausführung zu unterscheiden, bietet Ansatzpunkte, die im Abschnitt 4.3.2 aufgezeigten Schwachpunkte bei der Anwendung der FMEA zu beseitigen und die Interpretation der Versagensarten zu verbessern. Dazu wird der zwischen der Funktionsausführung und der Zweckbestimmung bestehende Ursache-Wirkungszusammenhang genutzt, der eine getrennte Durchführung der FMEA auf unterschiedlichen Ebenen erlaubt.

Auf der Ebene der Zweckbestimmung können ausgehend von der Funktionsdefinition die möglichen Ergebnisse der Funktionsausführung definiert werden. Es ist nicht nur die Angabe möglich, welche der Ergebnisse richtig und welche falsch sind, sondern darauf aufbauend auch, welche Folgen das Vorliegen eines falschen Ergebnisses in einer Situation haben kann, die ein anderes Ergebnis erfordert. Eine solchermaßen durchgeführte „Ergebnis-FMEA“ erlaubt die Angabe gefährlicher und hemmender Ergebnisse, die wegen der Entkopplung von der Funktionsausführung als generisch anzusehen sind. Ein späterer Funktionsträger muss so ausgelegt werden, dass zumindest die gefährlichen, und aus Gründen der Verfügbarkeit nach Möglichkeit auch die hemmenden Ergebnisse, mit einer hinreichenden Wahrscheinlichkeit keine fehlerhafte Funktionsausführung verursachen.

Um die Ursachen eines gefährlichen oder hemmenden Ergebnisses zu erklären, sind zu einem späteren Zeitpunkt auf der darunterliegenden Betrachtungsebene „Aktion / Tätigkeit“ die Fehler zu identifizieren, die bei der Funktionsausführung prinzipiell gemacht werden können. Entscheidend für die Identifizierung der bei der Funktionsausführung begehbaren Fehler wird das Prädikat sein, da es die Satzaussage liefert und die Aktion oder Tätigkeit beschreibt. Das Ergebnis einer „Prädikat-FMEA“ ist eine Liste fehlerhafter Aktionen oder Tätigkeiten, in deren Folge die mittels der „Ergebnis-FMEA“ identifizierten gefährlichen oder hemmenden Ergebnisse auftreten können. Im Unterschied zur stets als generisch aufzufassenden Ergebnis-FMEA können die identifizierten Fehler nur dann als generisch angesehen werden, wenn die betrachtete Aktion oder Tätigkeit als generisch definiert angesehen werden kann. Da eine generische Definition von Aktionen und Tätigkeiten nicht immer möglich ist, kann die Prädikat-FMEA nur in den entsprechenden Fällen generische Ergebnisse liefern.

In diesem hierarchischen FMEA-Schema kann die in der EN 60812 beschriebene Form der FMEA als „Subjekt-FMEA“ betrachtet werden. Wie im Abschnitt 4.3.1 beschrieben, zielt sie von ihrem Ansatz her auf bereits in der Entwicklung befindliche Systeme ab, d.h. über den Funktionsträger liegen bereits zumindest erste Realisierungsvorstellungen vor. Die dabei identifizierten Fehler und Ausfälle sind infolge dessen als realisierungsabhängig und nicht als generisch anzusehen. Bezogen auf die Ebene der Funktionsausführung sind die Fehler und Ausfälle Ursachen für die mit der Prädikat-FMEA identifizierten fehlerhaften Ausführungen.

Fazit

Grundsätzlich ist zu erwarten, dass sich auch die Gefährdungsidentifikation entsprechend der dreistufigen Struktur der Funktionsdefinitionen hierarchisch gliedern und sich über die jeweiligen Ergebnisse top-down verbinden lässt. In der Tabelle 16 werden die hierarchisch aufgebauten FMEA-Ebenen einschließlich ihrer Bezüge untereinander zusammengefasst.

Tabelle 16: Hierarchie der FMEA-Ebenen

Art	Ebene	Ergebnis der FMEA		Erläuterung
Ergebnis-FMEA	Zweckbestimmung	Gefährliche und hemmende Ergebnisse	Generisch	Erlaubt die Ableitung der prinzipiellen betrieblichen Folgen
Prädikat-FMEA	Funktionsausführung	Fehlerhafte Ausführungen; führen sie zu gefährlichen Ergebnissen, sind sie gefährlich	u.U. generisch	Liefert die Ursachen für gefährliche und hemmende Ergebnisse; nur dann generisch, wenn das Prädikat generisch definiert werden kann.
Subjekt-FMEA	Funktionsträger	Fehler und Ausfälle des Funktionsträgers, der zu fehlerhaften Funktionsausführungen führen	Nicht generisch	Liefert realisierungsabhängige Ursachen für fehlerhafte Funktionsausführungen; Kenntnis der Funktionsrealisierung erforderlich
HINWEIS: Einer fehlerhaften Ausführung können auch objektspezifische Fehler zugrunde liegen; das Objekt wird jedoch nicht als Teil der Funktion betrachtet → andere Funktionen sind für das nicht ordnungsgemäße Objekt verantwortlich.				

Der Bezug des hierarchisch aufgebauten dreistufigen FMEA-Ansatzes zur CENELEC-Sanduhr sowie der enge Zusammenhang zwischen der Funktionsdefinition und der Gefährdungsidentifikation wird im Bild 35 deutlich.

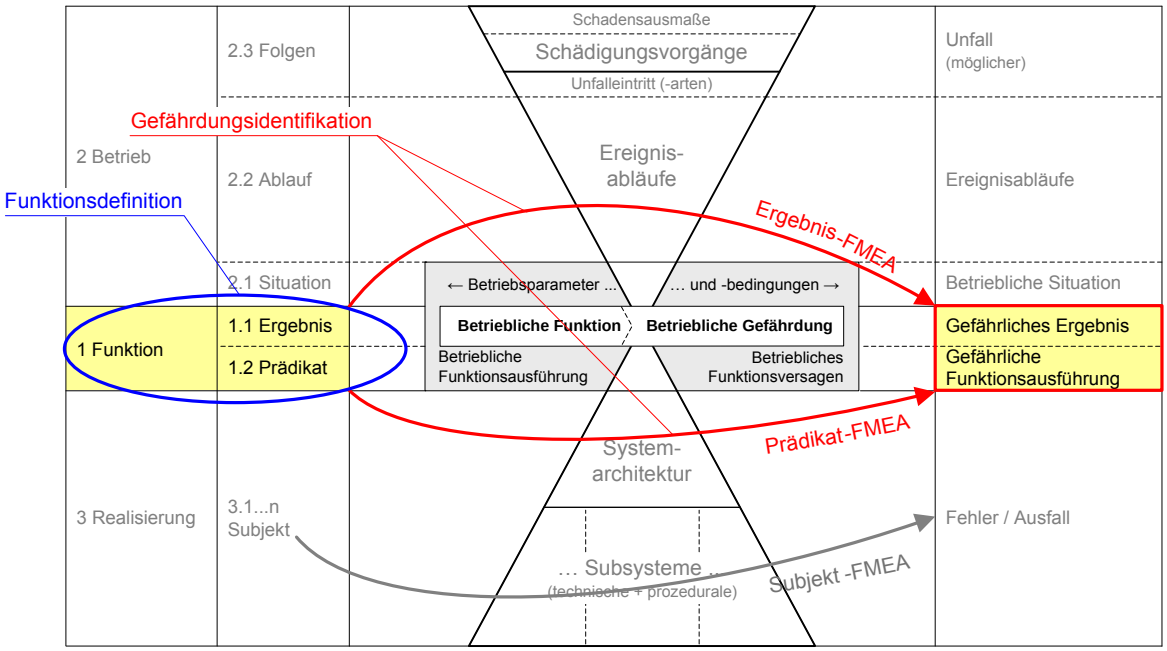


Bild 35: Einordnung des dreistufigen FMEA-Vorgehens in die CENELEC-Sanduhr

4.3.4 Konzept für eine Ergebnis-FMEA

Für die Entwicklung einer Ergebnis-FMEA, die der Identifizierung gefährlicher Ergebnisse dienen soll, ist zunächst zu klären, wodurch fehlerhafte Funktionsergebnisse charakterisiert sind, wann sie wie auf die funktionale Umgebung der versagenden Funktion wirken und wie sie systematisch identifiziert werden können.

4.3.4.1 Wahre, falsche und fehlende Ergebnisse

Der Betrieb eines Systems bedarf der kontrollierten Änderung der Zustände seiner Objekte. Ohne Zustandsänderungen würde das System unverändert in einer Ausgangsposition verharren. Die Zustandsänderungen werden durch spezifische Funktionen vorbereitet und herbeigeführt. Eine Funktion gilt als erfolgreich ausgeführt, wenn sie zu dem bezweckten Ergebnis geführt hat; ihr Ergebnis ist „wahr“. Ihre Ausführung war nicht erfolgreich, wenn das bezweckte Ergebnis nicht erreicht worden ist. Dies ist immer der Fall, wenn die Funktion zu einem

- nicht bezweckten Ergebnis oder
- zu keinem Ergebnis

führt. Für die Folgen eines nicht bezweckten Ergebnisses ist entscheidend, ob die nicht bezweckten Ergebnisse „erkannt“ werden oder „unerkannt“ bleiben. Werden sie „rechtzeitig“ erkannt, kann das System zu einer sicheren Seite reagieren. Der Betriebsablauf wird in diesem Fall gehemmt, aber nicht gefährdet. Bei einem zu „späten Erkennen“ oder einem

Unerkanntbleiben können hingegen Abläufe mit Unfallfolgen eintreten. Zwischen „erkannt“ und „unerkannt“ wird deshalb im Folgenden unterschieden:

- „erkannt“: rechtzeitig erkannt;
- „unerkannt“: zu spät oder nicht erkannt.

Da für die Einstufung eines Funktionsversagens als Gefährdung die Möglichkeit eines Unfalls maßgebend ist, müssen im Rahmen einer Gefährdungsidentifikation nur die „unerkannt“ vom bezweckten Ergebnis abweichenden Ergebnisse betrachtet werden.

Während sich „unerkannt falsche Ergebnisse“ relativ anschaulich als Werte oder Zustände auffassen lassen, die von den bezweckten Werten oder Zuständen abweichen, bedarf die Interpretation des ebenfalls nicht bezweckten Ergebnisses „unerkannt kein Ergebnis“ einer genaueren Betrachtung.

Was bedeutet „unerkannt kein Ergebnis“? Da Funktionen als Ergebnisse entweder Werte ausgeben oder Zustände erzeugen, werden folgende Situationen zunächst als mögliche Interpretationen von „kein Ergebnis“ aufgefasst und hinsichtlich ihrer Bedeutung analysiert:

- Es wird kein Wert ausgegeben;
- Es wird kein neuer Wert ausgegeben;
- Es wird kein Zustand erzeugt;
- Es wird kein neuer Zustand erzeugt.

Der Unterschied zwischen „kein Wert“ und „kein neuer Wert“ besteht darin, dass bei „kein neuer Wert“ ein alter Wert unerkannt weiterhin seine Gültigkeit behält. Wird z.B. das Anzeigen eines restriktiven Geschwindigkeitswechsels bezweckt, bedeutet „kein Ergebnis“, dass die bis zum Geschwindigkeitswechsel gültige höhere Geschwindigkeit vom System als weiterhin gültiger Wert aufgefasst wird. In der Folge würde vom Geschwindigkeitswechsel an mit einer zu hohen Geschwindigkeit gefahren. Statt „Kein Ergebnis“ liegt also in Wirklichkeit ein falscher Wert vor, der einer nachfolgenden Funktion als falscher Input dient. „Kein Ergebnis“ ist in diesem Fall als eine Ursache für „falscher Wert“ zu betrachten.

Im Fall einer Funktion „Gleisfreimeldung“ sind je nach Belegung des Gleises die Werte „frei“ oder „belegt“ zu erwarten. Bleiben beide Werte aus, liegt der nachfolgenden Funktion tatsächlich kein Wert als Input vor, sie kann und darf nicht ausgeführt werden. Das System wird in diesem Fall gehemmt, das Funktionsversagen offenbart sich. „Kein Wert“ kann somit nicht als „unerkannt“ angesehen werden.

Hinsichtlich einer Unterscheidung zwischen „kein Zustand“ und „kein neuer Zustand“ ist anzumerken, dass es sich bei „kein Zustand“ um eine irreale Betrachtung handelt, da es keinen Zustand der „Zustandslosigkeit“ geben kann. So wird bei Funktionen, die eine Zustandsänderung herbeiführen sollen, im Fall von „kein Ergebnis“ der alte Zustand vorliegen. Da er unerkannt vorliegt, ist „kein Ergebnis“ in diesem Fall gleichbedeutend mit „falscher Zustand“. Bei zustandsverändernden Funktionen kann also die Betrachtung „kein Ergebnis“ entfallen. Entweder ist das Ergebnis „wahr“ oder es ist „falsch“.

Im Bild 36 werden die vorstehenden Überlegungen zur Interpretation von „kein Ergebnis“ zusammengefasst.

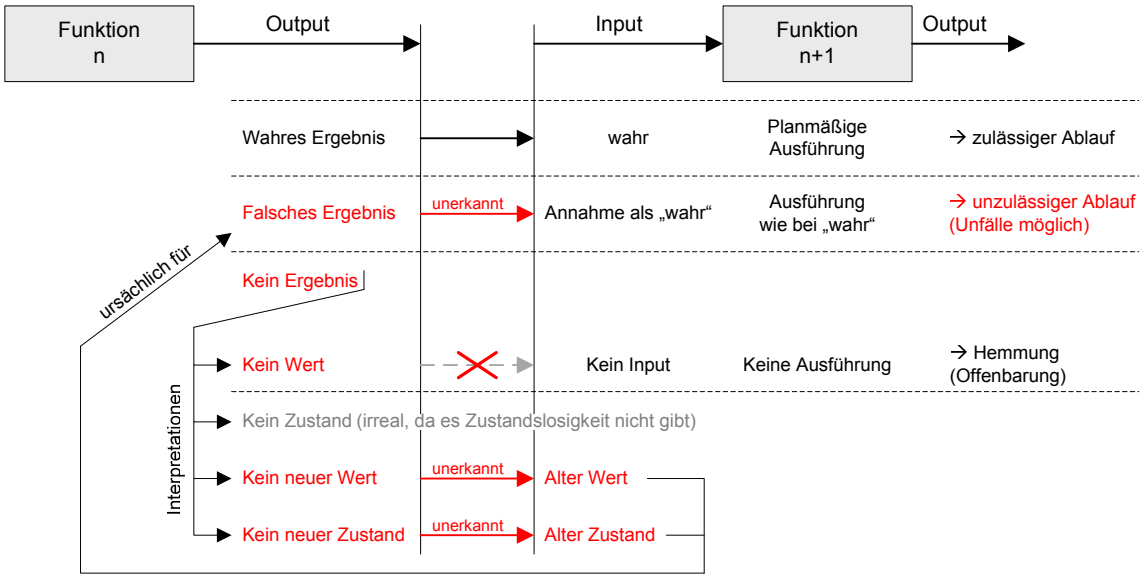


Bild 36: Interpretation von „Kein Ergebnis“

Fazit

- Bei Funktionen, deren Ergebnis eine Zustandsänderung sein soll, ist die Betrachtung „kein Ergebnis“ weder sinnvoll noch notwendig, da ein Zustand nur „wahr“ oder „falsch“ sein, nicht aber fehlen kann.
- Bei Funktionen, deren Ergebnis ein Wert ist, liegt nur dann „kein Ergebnis“ vor, wenn für eine nachfolgende Funktion der Input „leer“ ist, d.h. ohne Wert, bleibt. In diesem Fall offenbart sich allerdings das Versagen und das System wird gehemmt. In allen anderen Fällen ist „kein Ergebnis“ lediglich die Ursache für falsche Inputs, die bereits durch die Betrachtung „falsches Ergebnis“ erfasst werden.
- Entscheidend für die nach einem Funktionsversagen eintretenden Abläufe ist, ob bei einer nachfolgenden Funktion überhaupt ein Input ansteht und welchen Inhalts er ist. Eine Ergebnis-FMEA, die der Identifizierung gefährlicher Ergebnisse dienen soll, kann deshalb allein auf Basis der Betrachtung falscher Ergebnisse durchgeführt werden.
- Die Betrachtung von „kein Ergebnis“ ist im Rahmen einer Ergebnis-FMEA nicht erforderlich.

4.3.4.2 Ergebnisabweichungen

Die Abweichungen skalierbarer Funktionsergebnisse können durch „kleiner als“ oder „größer als“ ausgedrückt werden. Dies erlaubt eine einfache Ableitung falscher Ergebnisse aus den bezweckten Ergebniswerten.

Bei nicht skalierbaren Ergebnissen müssen inhaltliche Abweichungen betrachtet und definiert werden. Die einfachste Form der Abweichungsbestimmung ist die Negation. Wird z.B. das Erreichen einer bestimmten Weichenendlage „A“ bezweckt, ergibt sich das falsche Funktionsergebnis zu „Nicht A“. Darunter würden alle von „A“ abweichenden Weichenlagen subsumiert, d.h. „andere Endlage“ und „keine Endlage“. Da sich aus den beiden falschen Weichenlagen unterschiedliche Abläufe mit unterschiedlichen Unfällen ergeben können, ist es angebracht, die Wertabweichungen nicht durch die Negation des bezweckten Ergebnisses, sondern durch die Benennung der konkreten Ergebniswerte anzugeben.

Für die Ableitung der falschen nicht skalierbaren Ergebniswerte stehen als Eingangsinformationen die zweckorientierte Funktionsdefinition und die Angabe des mit der Funktion bezweckten Ergebnisses zur Verfügung. Diese Angaben beziehen sich auf ein von der Funktion zu behandelndes Objekt, so dass bei der Einbeziehung von Fachleuten und der Anschaulichkeit halber von einer möglichst vollständigen Beschreibung der nicht bezweckten Ergebnisse ausgegangen werden darf.

4.3.4.3 Identifizierung gefährlicher Ergebnisse mittels Ergebnissubstitution

Nicht alle Ergebnisabweichungen führen zu Unfällen und sind als gefährliche Ergebnisse einzustufen. Im Rahmen der Ergebnis-FMEA sollen die gefährlichen Ergebnisse identifiziert werden.

Zu jeder Funktion gibt es mindestens ein bezwecktes Ergebnis. Es ist das Ergebnis, das von der Funktion bei korrekter Ausführung als Output ausgegeben werden soll. Dieses Ergebnis wird als „wahr“ bezeichnet. Bei Funktionen, deren Ergebnis aufgrund unterschiedlicher Situationen verschiedene Erwartungswerte annehmen kann, kann entsprechend der vorliegenden Situation immer nur einer der Erwartungswerte „wahr“ sein. Das bedeutet, dass ein in einer Situation A wahres Ergebnis in einer Situation B falsch sein kann und umgekehrt. Im Rahmen der Gefährdungsidentifikation ist dies zu berücksichtigen.

I.d.R. ist eine Funktion in ein umgebendes funktionales System eingebunden, in welchem das ausgegebene Funktionsergebnis als Input weiterverwendet wird. Das umgebende funktionale System wird auf die jeweiligen Funktionsergebnisse mit Abläufen reagieren, die planmäßig beim Vorliegen wahrer Ergebnisse vorgesehen sind. Der Wahrheitswert des Funktionsergebnisses ist für das umgebende funktionale System jedoch nicht überprüfbar

und kann von ihm nur als „wahr“ angenommen werden.[28] Liegt ein falsches Funktionsergebnis vor, wird folglich auch dieses als „wahr“ aufgefasst und die beim Vorliegen wahrer Ergebnisse planmäßigen Abläufe folgen. Sie stehen allerdings im Widerspruch zu den tatsächlichen und durch das falsche Funktionsergebnis nicht richtig wiedergegebenen Verhältnissen. Aus diesen unerkannten Widersprüchen ergeben sich unplanmäßige Abläufe, die zu Unfällen führen können.

Ergebnissubstitution

Die bezweckten Ergebnisse ergeben sich unmittelbar aus der Funktionsdefinition. Im Rahmen der Ergebnis-FMEA ist zunächst für jedes der bezweckten Ergebnisse der im umgebenden funktionalen System planmäßig folgende Ablauf zu beschreiben. Anschließend wird das bezweckte Ergebnis durch die falschen Ergebnisse substituiert, die entsprechenden Versagen formuliert und deren Auswirkungen auf die Abläufe beschrieben. Besteht die Möglichkeit eines Unfalls, ist das entsprechende Ergebnis als gefährlich einzustufen. Im Einzelnen sind für eine generisch definierte Funktion im Rahmen der Ergebnis-FMEA folgende Schritte durchzuführen:

- Angabe des oder der mit dem definierten Funktionszweck bezweckten Ergebnisse;
- Beschreibung der beim Eintreten der Ergebnisse planmäßigen Reaktionen des umgebenden funktionalen Systems;
- Über die abgeleiteten Erwartungswerte hinaus die Angabe nicht bezweckter, aber denkbarer Ergebnisse;
- Substitution eines jeden bezweckten Ergebnisses durch alle von ihm abweichenden Ergebniswerte;
- Formulierung der durch die Ergebnissubstitutionen ausgedrückten Funktionsversagen;
- Beschreibung der mit den Funktionsversagen verbundenen unplanmäßigen Systemreaktionen im Hinblick auf die Möglichkeit von Unfällen.

[28] Mit der Überprüfung eines Funktionsergebnisses wird eine Reduktion der Versagenswahrscheinlichkeit der entsprechenden Funktion bezweckt. Das Vorsehen derartiger Überprüfungen ist ein diesem Ziel dienendes Realisierungsprinzip, mit dem kein über den eigentlichen Funktionszweck hinausgehender Zweck verfolgt wird. Deshalb kann in funktionaler Hinsicht eine Überprüfungsfunktion nur als Teil der Realisierung der betrachteten Funktion betrachtet werden. Ein funktionales System, das die betrachtete Funktion umgibt, kann aus diesem Grunde nicht die Ergebnisse der betrachteten Funktion überprüfen. So kann z.B. ein Triebfahrzeugführer den Wahrheitsgehalt eines ihm angezeigten Signalbegriffs nicht überprüfen. Er muss sich darauf verlassen können, dass das bei ihm eingehende Funktionsergebnis „wahr“ ist; der entsprechende Funktionsträger muss dementsprechend sicher „funktionieren“.

Substitutionstabelle

Die Ergebnis-FMEA mittels einer Ergebnissubstitution stellt ein sehr systematisches Vorgehen dar. Es kann in Form einer Tabelle übersichtlich und nachvollziehbar durchgeführt werden. Weitere, nachträglich erkannte „falsche“ Ergebnisse können leicht ergänzt werden. Tabelle 17 enthält ein Beispiel, wie eine solche Tabelle aufgebaut sein kann.

Tabelle 17: Beispiel für den Aufbau einer Ergebnis-Substitutionstabelle

Funktionsname					
Funktionszweck	Ausführung, um				
Funktionsergebnisse			**Identifikation gefährlicher Ergebnisse**		
Bezweckt	Output		Versagensformulierung	mögliche Abläufe	Beurt.
(a)	(b)	(c)	(d)	(e)	(f)
	W	„bezweckt“	÷		Planm.
	F				
	F				
	F				
	W	„bezweckt“	÷		Planm.
	F				
	F				
	F				
Hinweise					

Im Tabellenkopf werden der Funktionsname und der Funktionszweck angegeben. Sie sind der Funktionsdefinition zu entnehmen. Das oder ggf. die mit der Funktion bezweckten Ergebnisse werden in Spalte (a) eingetragen. In Spalte (c) werden jedem der bezweckten Ergebnisse die von ihm abweichenden Ergebnisse zugeordnet. Die Angaben „W“ und „F“ in Spalte (b) stehen für „wahr“ und „falsch“; in der jeweils ersten Zeile ist das bezweckte Ergebnis bereits als wahr gesetzt. Dies dient dem Beschreiben des planmäßigen Ablaufs in Spalte (e). Alle anderen Ergebnisse werden in die mit „F“ markierten Felder eingetragen, in der Spalte (d) jeweils die Versagen und in der Spalte (e) die daraus resultierenden Abläufe beschrieben. Die Versagen werden entsprechend der Abläufe in Spalte (f) als gefährlich oder hemmend beurteilt.

Es folgen drei Beispiele für Funktionen, deren Ergebnisse ein skalierbarer Wert (Bsp. 1), ein nicht skalierbarer Wert (Bsp. 2) und ein Zustand (Bsp. 3) sind.

Beispiel 1

Die Funktion „Trassierungstechnisch bedingte Geschwindigkeitsvorgabe wird ausgeführt, um geschwindigkeitsabhängige fahrdynamische Grenzen einzuhalten, die sich aus der Linienführung der Strecke ergeben. Die Funktion gibt als Ergebnisse skalierbare Werte aus.

Tabelle 18: Funktion mit einem skalierbarem Ergebnis (Substitutionstabelle)

Funktionsname		**„Trassierungstechnisch bedingte Geschwindigkeitsvorgabe“**			
Funktionszweck		Ausführung, um	trassierungstechnisch bedingte Grenzen einzuhalten.		
Funktionsergebnisse			**Identifikation gefährlicher Ergebnisse**		
Bezweckt	Output		Versagensformulierung	mögliche Abläufe	Beurt.
(a)	(b)	(c)	(d)	(e)	(f)
zul $V_{Strecke}$	W	„bezweckt“	÷	Fahrt mit ≤ zul $V_{Strecke}$	Planm.
	F	< zul $V_{Strecke}$	Es wird eine kleinere als die zulässige Geschwindigkeit vorgegeben.	Das Fahrzeug fährt u.U. langsamer als es erforderlich ist. → Hemmung (Fahrtzeitverlängerung)	Hem.
	F	> zul $V_{Strecke}$	Es wird eine größere als die zulässige Geschwindigkeit vorgegeben.	Das Fahrzeug fährt u.U. schneller als es zulässig ist. → Unfall (Entgleisung) möglich	Gef.
--	W	„bezweckt“	÷		Planm.
	F	--			
Hinweise					

Beispiel 2

Die Funktion „Gleisfreimeldung“ wird ausgeführt, um den Belegungszustand eines Gleises durch andere Fahrzeuge zu erfassen. Die Werte des Funktionsergebnisses sind nicht skalierbar. Als zweckspezifische Ergebniswerte können „frei von anderen Fahrzeugen“ und „Belegt von anderen Fahrzeugen“ angegeben werden. Weitere funktionsspezifische Ergebniswerte sind nicht vorstellbar. Die planmäßigen Systemreaktionen auf diese Werte sind „Fahrt“ und „Halt“. Weil beide Werte situativ „wahr“ sein können, werden sie jeweils in die Spalten „Bezweckt“ und „Output“ eingetragen.

Tabelle 19: Funktion mit zwei nicht skalierbaren Ergebnissen (Substitutionstabelle)

Funktionsname		**„Gleisfreimeldung“**			
Funktionszweck		Ausführung, um	den Zustand der Belegung eines Gleisabschnitts durch andere Fahrzeuge zu erfassen.		
Funktionsergebnisse			**Identifikation gefährlicher Ergebnisse**		
Bezweckt	Output		Versagensformulierung	mögliche Abläufe	Beurt.
(a)	(b)	(c)	(d)	(e)	(f)
„Frei von anderen Fahrzeu-gen“	W	„bezweckt“	÷	Zulassung einer Fahrt in ein freies Gleis.	Planm.
	F	„Belegt von anderen Fahrzeugen“	Obwohl das Gleis frei von anderen Fahrzeugen ist, wird eine Belegt-Meldung ausgegeben.	Die Fahrt wird nicht zugelassen. → Hemmung des Betriebs	Hem.
„Belegt von anderen Fahrzeu-gen“	W	„bezweckt“	÷	Keine Zulassung einer Fahrt.	Planm.
	F	„Frei von anderen Fahrzeugen“	Obwohl das Gleis von anderen Fahrzeugen belegt ist, wird eine Freimeldung ausgegeben.	Es wird eine Fahrt in ein belegtes Gleis zugelas-sen. → Unfall (Kollision) möglich	Gef.
Hinweise					

Beispiel 3

Die Funktion „Weiche umstellen“ wird ausgeführt, um die für eine Fahrt benötigte Solllage einer Weiche zu erreichen. Die Werte des Funktionsergebnisses sind nicht skalierbar. Als zweckspezifischer Ergebniswert ist „Solllage“ angegeben. Ist die Solllage erreicht, darf als Systemreaktion eine Fahrt erfolgen. Als denkbare, aber nicht bezweckte Ergebnisse können „Andere Endlage“ und „keine Endlage“ angeben werden.

Tabelle 20: Funktion mit einem nicht skalierbaren Ergebnis (Substitutionstabelle)

Funktionsname	**„Weiche umstellen“**				
Funktionszweck	Ausführung, um	die für eine Fahrt benötigte Solllage einer Weiche zu erreichen.			
Funktionsergebnisse			**Identifikation gefährlicher Ergebnisse**		
Bezweckt	Output		Versagensformulierung	mögliche Abläufe	Beurt.
(a)	(b)	(c)	(d)	(e)	(f)
Solllage	W	„bezweckt“	÷	Fahrt in das planmäßige Gleis	Planm.
	F	Andere Endlage	Statt der Solllage liegt eine andere Endlage vor.	Fahrt in ein anderes Gleis / über den anderen Strang → Unfall, z.B. Kollision oder Entgleisung	Gef.
	F	Keine Endlage	Statt der Solllage liegt keine Endlage vor	Fahrt in die unvollständig gestellte Weiche → Unfall, Entgleisung in der Weiche	Gef
--	W	„bezweckt“	÷	--	Planm.
	F	--		--	--
Hinweise					

4.4 Funktionsgrundtypen

Funktionen besitzen Zweckbestimmungen und Wirkungsweisen, die unterschiedlich stark differieren. Für Funktionen, die bestimmte Ähnlichkeiten aufweisen, können Funktionsgrundtypen definiert werden. Sie lassen sich aus grundsätzlichen Motivationen ableiten. Dem originären Zweck eines Verkehrssystems entsprechend ist dies zuvorderst die Erfüllung der Verkehrsaufgabe. Dies möglichst sicher zu tun und nach Möglichkeit zur Verbesserung der Sicherheit in die sicherheitliche Wirkungskette einzugreifen, stellt eine weitere Motivation dar. Da grundsätzlich die Anforderung besteht, den Betrieb der Eisenbahnen sicher zu führen, sind die diesen beiden Motivationen entsprechenden Funktionen innerhalb der Betriebsverfahren eng miteinander verbunden. Sie bilden quasi den Kern und werden in den

Abschnitten 4.4.1 und 4.4.2 näher betrachtet. Aber auch die Verbesserung der Effizienz, mit der der Betrieb geplant und durchgeführt wird, kann Motivation für die Realisierung entsprechender Funktionen sein, die den Kern ergänzen. Sie werden im Rahmen dieser Arbeit nicht betrachtet.

4.4.1 Erfüllung der Verkehrsaufgabe

Der Zweck eines Verkehrssystems liegt in der Erfüllung einer Verkehrsaufgabe, die in der Ortsveränderung von Personen und Gütern besteht. Dazu müssen bestimmte Funktionen ausgeführt werden, die sich aus den Systemeigenschaften des Verkehrssystems und jener der zu transportierenden Personen und Güter ergeben. Die entsprechenden Funktionen können anhand bestimmter, i.d.R. für alle spurgeführten Verkehrssysteme elementarer Vorgänge, wie z.B. dem Bewegen von Fahrzeugen auf der Infrastruktur, der Zuweisung der zu befahrenden Infrastruktur und dem Stellen beweglicher Fahrwegelemente, beschrieben werden.

Die übergeordneten betrieblichen Funktionen werden durch aufeinander abgestimmte betriebliche Regeln und technische Hilfsmittel realisiert, die als Teile der betrieblichen Funktionen aufgefasst werden können. Der unmittelbare Zweck dieser Subsystemfunktionen besteht nicht mehr in der Erfüllung der Verkehrsaufgabe, sondern in einem funktionalen Beitrag zu einer betrieblichen Funktion, die der Erfüllung der Verkehrsaufgabe dient. Erst durch die Zuordnung zu der betrieblichen Funktion kann der Bezug zum Betriebsprozess hergestellt werden. Beispiel: Für eine Funktion, deren unmittelbarer Zweck die „Ermittlung des Fahrzeugorts“ ist, kann der Bezug zum Betriebsprozess erst durch eine Zuordnung zu einer betrieblichen Funktion, wie z.B. „Ermittlung der Belegung des zu befahrenden Gleises durch andere Fahrzeuge“ oder „Einhalten der vorgegebenen Geschwindigkeit“, angegeben werden.

4.4.2 Verbesserung der Sicherheit

Trotz des Bestrebens betriebliche Funktionen bereits durch eine geeignete Realisierung ihrer Funktionsträger möglichst sicher auszuführen, sind in allen Verkehrssystemen Einrichtungen zu finden, die zur Verbesserung der Sicherheit eingeführt worden sind. Sie werden nicht unmittelbar für die Durchführung der Verkehrsaufgabe, sondern nur zur Reduzierung des damit in Verbindung stehenden Risikos benötigt. So sind beispielsweise im Eisenbahnwesen Einrichtungen zur Überwachung der von Triebfahrzeugführern vorgenommenen Geschwindigkeitsregelung und zur Führung entgleister Fahrzeuge bekannt. Die Luftfahrt kennt Kollisionswarneinrichtungen; im Automobilsektor dienen Sicherheitsgurte, Airbags und Systeme zur Stabilisierung des Fahrverhaltens der Reduzierung des Risikos.

Die Systeme unterscheiden sich nicht nur hinsichtlich ihrer Realisierung, sondern greifen auch in unterschiedlicher Weise in die Systemsicherheit ein. Diese Eingriffe können systematisch unterschieden und die entsprechenden Zielsetzungen im Sinne einer überge-

ordneten Zweckbestimmung beschrieben werden. Aus der in 3.1.1 beschriebenen Wirkungskette und der in 3.1.2 definierten wirkungskettenorientierten Darstellung der Risikoformel ergeben sich bezüglich der Sicherheit drei Eskalationsstufen:

- Vom Eintreten von Fehlern und Ausfällen bis zum Eintritt einer Gefährdung,
- vom Eintritt einer Gefährdung bis zum Unfalleintritt,
- vom Unfalleintritt bis zum vollen Schadensausmaß.

Funktionen, die der Verbesserung der Sicherheit dienen sollen, müssen folglich dem Ziel dienen, den Eintritt der jeweils nächsten Eskalationsstufe zu verhindern. Dies kann durch folgende Ziele ausgedrückt werden:

- Überwachung auf Fehler / Ausfälle bei der Ausführung einer Funktion,
- Abfangen einer eingetretenen Gefährdung, um den Unfalleintritt zu verhindern,
- Begrenzung des Schadensausmaßes im Falle des Unfalleintritts.

Überwachung auf Fehler und Ausfälle

Überwachungseinrichtungen haben die Funktion, die korrekte Ausführung einer Grundfunktion zu „überwachen“ und ggf. einzugreifen; sie führen die Grundfunktion nicht aus. Mit Überwachungseinrichtungen können die Gefährdungsraten der Grundfunktionen gesenkt werden. Sie werden häufig so realisiert, dass sie die Einhaltung sicherheitsrelevanter Parameter einer Grundfunktion überwachen und gegebenenfalls die Einhaltung erzwingen, indem eine Reaktion zur sicheren Seite ausgelöst wird. Deshalb wird auf der betrieblich-funktionalen Betrachtungsebene die entsprechende Einrichtung nicht als eigenständige Funktion, sondern als ein Bestandteil der Realisierung der jeweiligen Grundfunktion betrachtet.

Abfangen eingetretener Gefährdungen

Abfangfunktionen haben die Aufgabe, nach dem gefährlichen Versagen einer Grundfunktion die Übergangswahrscheinlichkeit zu einem Unfall zu verringern. Sie wirken innerhalb der Ereignisabläufe als planmäßige Barrieren. Eine Abfangfunktion wird dann erforderlich, wenn die für eine Grundfunktion vorgegebene Gefährdungsrate weder durch die direkte Realisierung der Grundfunktion noch in Kombination mit einer Überwachungseinrichtung eingehalten werden kann.

Abfangfunktionen sind häufig so realisiert, dass sie während des planmäßigen Betriebs vorbereitet, eingestellt oder angestoßen werden. Die beabsichtigte Wirkung tritt erst im Zusammenhang mit dem Versagen von Grundfunktionen ein. Beispiel: Flankenschutzweichen und Gleissperren fangen die Gefährdungen ab, die beim Versagen der Grundfunktionen Geschwindigkeitseinhaltung oder Stillstandsicherung eintreten.

Begrenzung des Schadensausmaßes

Schadenbegrenzungsfunktionen haben die Aufgabe, nach einem Unfall das Schadensausmaß zu begrenzen. Beispiel: Mit Führungsschienen sollen entgleiste Fahrzeuge dicht am eigentlichen Lichtraumprofil geführt werden, um das Ausmaß von Kollisionen mit anderen Fahrzeugen, Brücken usw. möglichst gering zu halten.

4.4.3 Einfluss auf das Risiko

Die identifizierten Funktionsgrundtypen „Betriebliche Funktion“, „Subsystemfunktion“, „Prüf- und Kontrollfunktion“, „“Abfangfunktion“ und „Schadenbegrenzungsfunktion“ können entsprechend ihrer Zweckbestimmungen und Wirkungsweisen der Sanduhr zugeordnet werden (Bild 37).

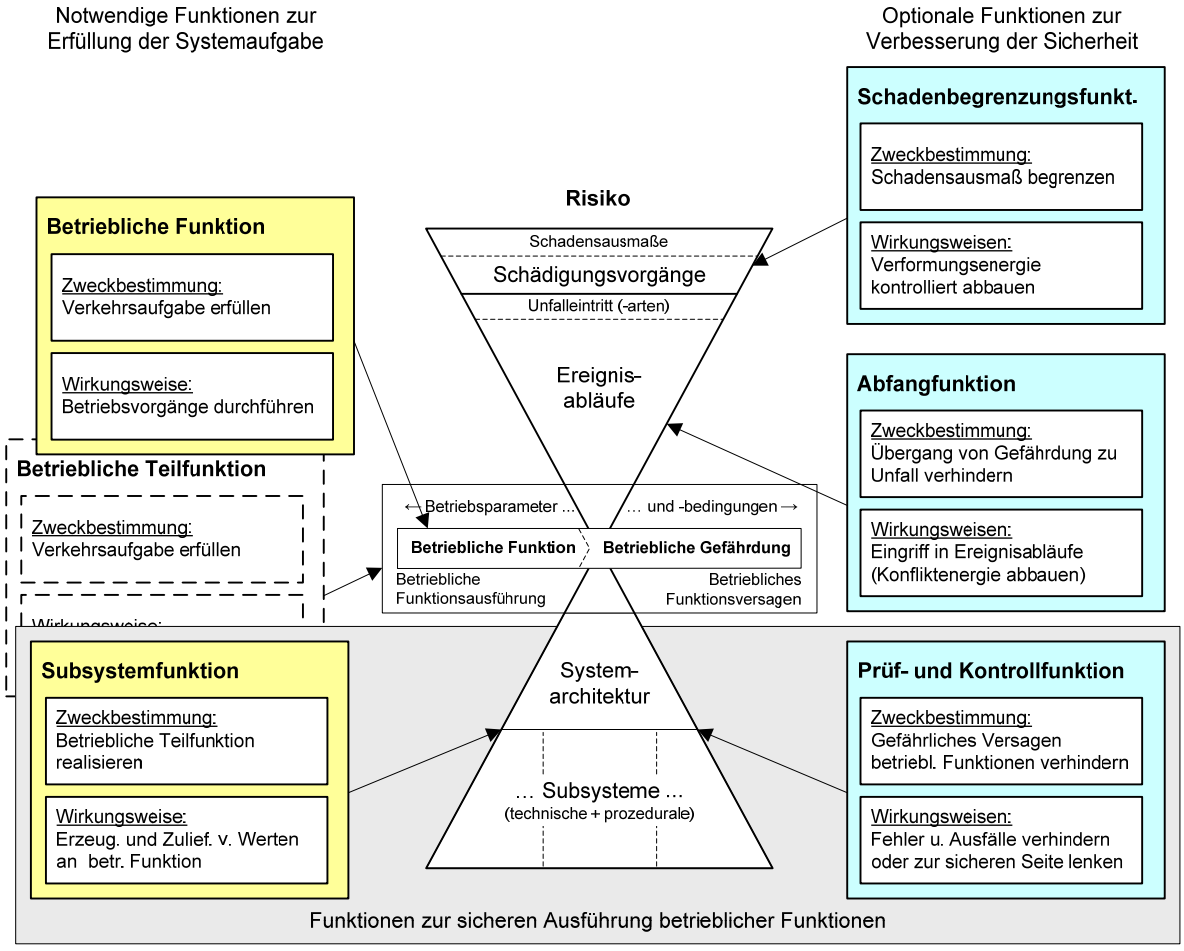


Bild 37: Zuordnung der übergeordneten Funktionszwecke zur CENELEC-Sanduhr

Die betrieblichen Funktionen können u.U. in betriebliche Teilfunktionen aufgeteilt werden. Bis zu welchem Detaillierungsgrad dies unter Wahrung des generischen Anspruchs möglich sein wird, ist Gegenstand weiterer Forschungsaktivitäten. Der entsprechende Block wird deshalb ohne Farbe und nur gestrichelt dargestellt.

4.4.4 Tabellarische Übersicht

Tabelle 21: Elementare Funktionstypen

Funktionstyp	Zweckbestimmung	Wirkungsweise	Merkmale
Betriebliche Funktion	Verkehrszweck erfüllen	Betriebsvorgänge durchführen	Unmittelbarer Bezug zu Betriebsprozessen erkennbar (Fahrten, zugehörige Fahrwegeinstellung und –sicherung)
Betriebliche Teilfunktion		Wie betriebliche Funktion	Für sich allein kein Bezug zum Betrieb erkennbar, d.h. der Bezug ergibt sich erst über die Angabe einer betrieblichen Funktion. Beispiel: Liefern einer Ortsinformation für eine Funktion, die der Gleisfreimeldung dient. Ihr Versagen kann die Ursache einer betrieblichen Gefährdung sein.
Subsystemfunktion	Betriebliche Funktion / Betriebliche Teilfunktion realisieren	Erzeugung und Zulieferung von Daten an betriebliche Funktion	Zweck wird in einer übergeordneten Systemarchitektur durch Festlegung von Subsystemen determiniert
Prüf- und Kontrollfunktion	Gefährliches Versagen betrieblicher Funktionen verhindern	Fehler und Ausfälle bei der Ausführung von Subsystemfunktionen werden verhindert oder detektiert und eine Reaktion zur „sicheren Seite“ ausgelöst	Optional, um für eine betriebliche Funktion eine vorgegebene Gefährdungsrate einzuhalten. Es ist stets eine zugehörige Funktion vom Typ Subsystemfunktion angebbar, beide sind Teil einer betrieblichen Funktion; Ihr Versagen erhöht die Wahrscheinlichkeit des Eintretens der Gefährdung, die sie verhindern soll;.
Abfangfunktion	Übergang von Gefährdung zu Unfall verhindern	Kinetische Konfliktenergie abbauen / trennen	Optional; kann erforderlich werden, wenn trotz des Einhaltens einer vorgegebenen Gefährdungsrate das resultierende Risiko zu hoch ist.
Schadenbegrenzung **„Schadenbegrenzungsfunktion“**	Schadensausmaß begrenzen	Verformungsenergie kontrolliert abbauen	Optional; kann erforderlich werden, wenn trotz des Einhaltens einer vorgegebenen Gefährdungsrate das resultierende Risiko zu hoch ist.

4.4.5 Umgang mit den Begriffen „Sicherheitsfunktion“ und „Schutzfunktion“

Im Anwendungsgebiet sind auch die Begriffe Sicherheitsfunktion und Schutzfunktion verbreitet. Sie haben in die Systematik der Funktionsgrundtypen keinen Eingang gefunden. Der Begriff „Sicherheitsfunktion“ erweist sich als zu unspezifisch, um als generisch gelten zu können. Er kann im Rahmen einer generischen Referenz keine Anwendung finden. Der Begriff „Schutzfunktion“ findet sich nicht im von MASCHEK in [MAS09] übergeordnet formulierten Sinne wieder, sondern wird entsprechend der Wirkungskette in einer verfeinerten Abstufung verwendet. Auf beide Begriffe wird in den beiden folgenden Unterabschnitten eingegangen.

4.4.5.1 Sicherheitsfunktion

Der Begriff „Sicherheitsfunktion“ wird in zahlreichen Normen und Veröffentlichungen verwendet. MILIUS hat die entsprechenden Quellen detailliert untersucht und kommt in [MIL09, S. 47] zu dem Ergebnis, dass *„die in den Normen gegebenen Sicherheitsfunktionen für eine praktische Anwendung zu wenig spezifisch scheinen,“* und diskutiert drei Optionen zur Definition des Begriffs „Sicherheitsfunktion“:

- *„Alle Funktionen, aus denen Gefährdungen […] resultieren, werden als Sicherheitsfunktionen bezeichnet.*
- *Alle Funktionen, an die im Rahmen des Sicherheitsnachweises qualitative und/oder quantitative Anforderungen gestellt werden,* [!] *bzw. für die im Sicherheitsnachweis Annahmen getroffen werden, werden als Sicherheitsfunktionen bezeichnet.*
- *Alle Funktionen, für die eine zulässige Gefährdungsrate kleiner als 10^{-5} Gefährdungen pro Stunde (SIL 1) gefordert wird, werden als Sicherheitsfunktionen bezeichnet.“*

Die Einstufung aller Funktionen, aus denen sich Gefährdungen ergeben können, ist, wie auch MILIUS schlussfolgert, zu unspezifisch, da jede Funktion, die einen Einfluss auf die Fahrzeugbewegungen hat, ein theoretisches Gefährdungspotenzial besitzt.

Die Einstufung aller Funktionen als Sicherheitsfunktionen, an die im Rahmen des Sicherheitsnachweises bestimmte Anforderungen gestellt werden, setzt zunächst eine Analyse zur Bestimmung der Anforderungen voraus. Eine Funktion würde in Abhängigkeit von den Ergebnissen der Analyse in einem Fall als Sicherheitsfunktion und in einem anderen Fall nicht als Sicherheitsfunktion betrachtet werden.

Auch die Einstufung aller Funktionen als Sicherheitsfunktion, für die eine fest definierte zulässige Gefährdungsrate gefordert wird, würde das Problem einer fallabhängigen Einstufung nicht lösen.

Die Verwendung des Begriffs „Sicherheitsfunktion“ ist mit dem Anspruch, Funktionen generisch definieren und klassifizieren zu wollen, nicht vereinbar. Ein generischer Funkti-

onsgrundtyp „Sicherheitsfunktion“ ist nicht definierbar. Der Begriff „Sicherheitsfunktion“ kann deshalb bei der Definition generischer Funktionen keine Anwendung finden. [29]

4.4.5.2 Schutzfunktion

MASCHEK stellt in [MAS09] ein Modell für *„eine generische Sicht auf die Betriebssicherheit im spurgeführten Verkehr“* vor. Im Zentrum seiner Betrachtungen stehen die Betriebssicherheit sowie das Herleiten von Funktionen, mit denen die Sicherheit des Betriebs gewährleistet werden soll. Kern des Modells ist der *„Regelkreis der Betriebssicherheit“*, in dem dargestellt wird, wie bestimmte Komponenten funktional zusammenwirken müssen, um die geforderte Sicherheit zu erzeugen. Ausgehend von den zwei maßgebenden Systemeigenschaften, den langen Bremswegen durch geringe Haftreibung und der Spurführung, wird die Zweckbestimmung der betrachteten Funktionen in der Vermeidung von Kollisionen und Entgleisungen gesehen.[30] Daraus wird der Begriff „Schutzfunktion“ abgeleitet und für die betrachteten Funktionen eingeführt. Er wird zwar nicht explizit definiert, wird aber im Kontext der Veröffentlichung vom Verfasser dieser Arbeit wie folgt verstanden: Schutzfunktionen sind Funktionen, die dem Zweck dienen, bestimmte ungewollte Ereignisse zu verhindern. So verstanden, werden die unter dem Begriff „Schutzfunktionen“ subsumierten Funktionen durch die in den Abschnitten 4.4.1 bis 4.4.4 definierten Funktionsgrundtypen abgedeckt. Die damit einhergehende Klassifizierung der Schutzfunktionen spiegelt nicht nur die bezweckten Schutzziele, sondern auch die unterschiedlichen Wirkungsweisen und Einflussnahmen auf die Sicherheit wieder (vgl. a. Bild 35). So dienen Prüf- und Kontrollfunktionen dem Schutz vor Gefährdungen, die durch Ausfälle und Fehler hervorgerufen werden. Abfangfunktionen dienen dem Schutz vor den Folgen von Gefährdungen und Schadensbegrenzungsfunktionen dienen dem Schutz vor Unfallfolgen. Funktionen, die dem Schutz vor dem Überschreiten physikalischer Grenzen und dem Schutz vor Kollisionen mit anderen Fahrzeugen, Dritten oder sonstigen Hindernissen dienen, sind für die Betriebsführung eines jeden Verkehrssys-

[29] Unabhängig von der Entscheidung, den Begriff „Sicherheitsfunktion“ nicht im Zusammenhang mit generischen Beschreibungen zu verwenden, ist zu überlegen, ob in den Normen statt des Begriffs „Sicherheitsfunktion“ nicht besser der Begriff „sicherheitsrelevante Funktion“ verwendet werden sollte. Eine Funktion wäre dann als sicherheitsrelevant einzustufen, wenn die an sie gestellten Anforderungen oberhalb eines bestimmten Wertes lägen.

[30] Aus einer mehr generischen Sichtweise ist anzumerken, dass sich in allen Verkehrssystemen unabhängig von der Länge des Bremswegs Kollisionen ereignen können. Einzige Voraussetzungen sind das zeitgleiche Bewegen mehrerer Fahrzeuge auf einer Verkehrsinfrastruktur, das höhengleiche Kreuzen systemfremder Verkehrsteilnehmer oder das Hineingelangen systemfremder Objekte in den Lichtraum. Die Kollisionsvermeidung ist somit in jedem Verkehrssystem zu Land, Wasser und in der Luft ein elementares Schutzziel. Die Systemeigenschaft „Lange Bremswege durch geringe Haftreibung“ ist lediglich eine Randbedingung, die dazu geführt hat, dass die Eisenbahn zur Erfüllung dieses Schutzziels verhältnismäßig komplexe betriebliche Regeln bereithalten sowie einen mehr oder minder großen technischen Aufwand betreiben muss.

tems elementar. Sie werden den betrieblichen Funktionen bzw. deren Teilfunktionen zugeordnet.

Der in [MAS09] verwendete Begriff “Schutzfunktionen” ist ein Oberbegriff für Funktionen, die unterschiedlichen Funktionsgrundtypen zugeordnet werden können. Er kann deshalb für die Klassifizierung der zu definierenden Funktionen nicht herangezogen werden.

4.5 Formular für das Definieren generischer Funktionen und Gefährdungen

4.5.1 Zweck

In den Abschnitten 4.2 bis 4.4 sind Anforderungen an das Formulieren generischer Funktionen, ein Weg zur Identifizierung gefährlicher Ergebnisse und Möglichkeiten zur Klassifizierung der Funktionen beschrieben worden. Diese Schritte sollen für alle Funktionen möglichst einheitlich durchgeführt werden. Formulare erlauben i.d.R. ein systematisches Vorgehen und unterstützen die angestrebte einheitliche Umsetzung. Ihre Rubriken können zudem als Grundlage für das Ablegen der Informationen in einer Datenbank herangezogen werden. Das Formular ist in diesem Sinne auch als ein Vorläufer für eine entsprechende Eingabemaske zu verstehen. Die Entwicklung und Umsetzung einer solchen Datenbank ist nicht Gegenstand dieser Grundlagenarbeit.

4.5.2 Zu erfassende Inhalte

Das Definieren generischer Funktionen und Gefährdungen gliedert sich in zwei aufeinander aufbauende Bearbeitungsschritte. Der erste Schritt dient der Definition und Einordnung der Funktion. Im zweiten Schritt, der Ergebnis-FMEA, wird die Identifizierung der falschen und insbesondere der darunter gefährlichen Ergebnisse vorgenommen. Dazu werden einige der im ersten Schritt erfassten Inhalte übergeben.

Schritt 1: Name, Definition und Einordnung

Die zu erfassenden Inhalte ergeben sich aus dem Ziel, betriebliche Funktionen generisch beschreiben und definieren sowie die entsprechenden Gefährdungen identifizieren zu wollen. Den Ausgangpunkt soll gemäß der in 4.2.4 aufgestellten Anforderungen die Angabe des Zwecks bilden, der mit der Ausführung einer Funktion erreicht werden soll. Das bezweckte Ergebnis (Output) steht damit unmittelbar im Zusammenhang. Seine Angabe präzisiert den Zweck und grenzt die Funktion gegenüber anschließend ablaufenden Funktionen ab. Zugleich bildet das bezweckte Ergebnis den Ausgangspunkt für die Identifizierung der gefährlichen Ergebnisse (vgl. a. 4.3.4). So, wie der Output die Funktion gegenüber den nachfolgenden Funktionen abgrenzt, können durch die Angabe des Inputs auch

die zuvor ablaufenden Funktionen abgegrenzt werden: Alles, was als Input angegeben wird, wird nicht durch das Ausführen der zu definierenden Funktion erzeugt.[31]

Um die sich aus der Zweckbestimmung und dem Out- und dem Input ergebende Definition inhaltlich zu untermauern, wird ferner eine Einordnung der Funktion in den betrieblichen Kontext vorgenommen. Sie besteht aus einer Beschreibung des Bezugs der Funktion zum Betriebsprozess und einer Klassifizierung entsprechend der in 4.4 beschriebenen Funktionsgrundtypen.

In der Tabelle 22 werden die im ersten Schritt zu erfassenden Inhalte aufgeführt, erläutert und die Eingabefelder des Erfassungsformulars angegeben. Im Anhang 9 wird ein Beispiel für die Umsetzung gegeben.

Tabelle 22: Zu erfassende Inhalte

Inhalte und Erläuterungen			**Eingabefelder**
Name	Funktionsnummer	Optionale Angabe, die zu Ordnungszwecken angeben werden kann.	„Nummer“
	Funktionsname	Der Funktionsname soll eine einfache Benennung der Funktion erlauben, jedoch nicht die Definition ersetzen.	„Funktionsname“
Definition	Die Funktionsdefinition ergibt sich aus der Zweckbestimmung und dem damit verbundenen Ergebnis. Durch die Angabe des Inputs wird die Funktion gegenüber anderen Funktionen abgegrenzt.		
	Zweckbestimmung	Es soll keine Aktion oder Tätigkeit, sondern der Zweck beschrieben werden. Dies kann durch die Formulierung einer adverbialen Bestimmung des Zwecks als Finalsatz unterstützt werden, die mit den Worten „Ausführung, um …“ eingeleitet wird.	Eingeleitet mit „Ausführung, um“
	Ergänzende Erläuterung	In dieses Feld können über die Zweckbestimmung hinausgehende Angaben gemacht werden, wie z.B. Hinweise auf Subfunktionen der definierten Funktionen.	„Ergänzende Erläuterung“

Fortsetzung der Tabelle auf der folgenden Seite

[31] Die Nutzung des Out- und Inputs generischer Funktionen zum Bilden eines in sich geschlossen generischen Systemmodells und zur Prüfung der Vollständigkeit desselben wird in dieser Arbeit nicht betrachtet. Im Rahmen laufender Forschungsaktivitäten soll u.a. geklärt werden, inwieweit es allgemeine Zwangsläufigkeiten in der Abfolge der Funktionen gibt. So wird beispielsweise beim FunkFahrBetrieb im Gegensatz zu vielen anderen Systemrealisierungen das Stellen der Weichen erst nach dem Erteilen der Erlaubnis zum Befahren eines Abschnitts vorgenommen. Generische Modelle werden deshalb bei der Abbildung von Funktionsabfolgen entsprechende Freiheitsgrade bieten müssen.

Inhalte und Erläuterungen			Eingabefelder
	Output (bezwecktes Ergebnis)	Das bezweckte Ergebnis steht in einem unmittelbaren Zusammenhang mit der Zweckbestimmung. I.d.R. wird es ein oder zwei bezweckte Ergebniswerte geben, auf die bestimmte zulässige betriebliche Abläufe folgen. Für einen dritten Ergebniswert wird als Reserve entsprechende Felder vorgesehen.	je „Ergebnis“, die Felder „Ergebniswert“, „Zulässige betriebliche Folge“
	Input	Mit der Angabe des Inputs wird die Funktion gegenüber anderen Funktionen abgegrenzt. Wegen der generischen Betrachtungsweise ist die Herkunft des Input für die Definition der Funktion unerheblich. Das Formular muss ggf. für weitere Inputs erweiterbar sein.	„Input 1“, „Input 2“, „Input 3“ ggf. weitere Felder
Einordnung	Die Einordnung der Funktionen soll entsprechend der im Abschnitt 4.4 definierten Funktionsgrundtypen erfolgen. Der Betriebsprozess bildet die Bezugsebene für die Klassifizierung.		
	Bezug zum Betriebsprozess	Der Bezug zum Betriebsprozess ist zu erläutern. Dies soll der Vorbereitung der Klassifizierung dienen, dem Bearbeiter aber auch eine Art Plausibilitätsprüfung für die unter „Definition“ gemachten Angaben bieten, da die Definition und die Einordnung widerspruchsfrei sein müssen.	„Bezug zum Betriebsprozess“
	Klassifizierung	Die Klassifizierung erfolgt für die Grundtypen „betriebliche Funktion“, „betriebliche Teilfunktion“, „Abfangfunktion“ und „Schadenbegrenzungsfunktion“. Sie liegen im Sanduhr-Modell (vgl. a. 3.1.5 u. 4.4) auf bzw. oberhalb der Betriebsebene. Ferner wird für übergeordnete Definitionen die Einstufung als „Funktionsgruppe“ vorgesehen	4 Ankreuzfelder mit Merkmalen der Grundtypen 1 Ankreuzfeld „Andere“ 1 Ankreuzfeld „Funktionsgruppe“
Anmerkungen / Bearbeitungshinweise		Für Informationen, die keinem der anderen Eingabefelder zugeordnet werden können, sollte ein universelles Eingabefeld zur Verfügung stehen. Darin können z.B. Anmerkungen zur Funktion oder zum Stand der Bearbeitung aufgenommen werden.	„Anmerkungen / Bearbeitungshinweise“

Schritt 2: Gefährdungsidentifikation

Im zweiten Schritt sollen im Rahmen einer Ergebnis-FMEA die gefährlichen und hemmenden Ergebnisse ermittelt werden, die beim Versagen der Funktionsausführung eintreten können. Sie sind, im Gegensatz zu den in einer bestimmten betrieblichen Situation bezweckten „wahren“ Ergebnissen, „falsch“. Als „falsch“ gelten nicht nur die grundsätzlich nicht

bezweckten Ergebnisse, sondern auch jene der bezweckten Ergebnisse, die in einer anderen als der geplanten betrieblichen Situation auftreten (vgl. a. 4.3.4.3).

Auch das unter 4.3.4.3 vorgestellte Vorgehen, bei dem die bezweckten Ergebniswerte systematisch durch falsche Ergebniswerte substituiert werden, ist tabellarisch ausgebaut und kann in ein entsprechendes Formular umgesetzt werden. Sein struktureller Aufbau ist mit der im Abschnitt 4.3.4.3 dargestellten Tabelle 17 identisch.

Aus dem ersten Schritt werden die bezweckten Ergebnisse übernommen. Die grundsätzlich nicht bezweckten Ergebnisse sind entsprechend 4.3.4.2 zu ermitteln und einzutragen. Die wahren, d.h. die bezweckten Ergebnisse, und die falschen Ergebnisse werden in der Tabelle gegenübergestellt. Zu jedem dieser so erzeugten Widersprüche ist das Versagen zu formulieren und anhand der möglichen unplanmäßigen Betriebsabläufe und deren Folgen die Einstufung als „gefährlich“ oder „hemmend“ vorzunehmen.

Ob ein Input „wahr“ oder „falsch“ ist, wird bei der Analyse nicht berücksichtigt, da sein Wahrheitswert nicht durch die zu definierende, sondern durch die ihn erzeugende, d.h. eine andere Funktion beeinflusst wird. Für die Gefährdungsidentifikation der zu definierenden Funktion wird der Input stets als „wahr“ angenommen (vgl. a. Fußnote 28).

Bei EDV-gestützter Arbeitsweise können die wahren und falschen Ergebnisse automatisch gegenübergestellt werden. Für den Bearbeiter ergibt sich dadurch ein „Zwang“, zu jedem der erzeugten Widersprüche mit einer Versagensformulierung, einer Ablaufbeschreibung und einer Einstufung „Stellung zu nehmen“. Gleiches gilt, wenn im Rahmen neuerer Erkenntnisse für eine Funktion weitere bezweckte oder nicht bezweckte Ergebnisse nachgetragen werden. Im Anhang 9 wird ein Beispiel für eine Eingabemaske zur Gefährdungsidentifikation gegeben, in der in den grau unterlegten Feldern die bei der Definition gemachten Angaben übernommen werden und darauf basierend die weiß hinterlegten Felder auszufüllen sind.

4.5.3 Umsetzung

Im Rahmen dieser Arbeit sind entsprechend der beiden Bearbeitungsschritte zwei einfache Eingabemasken für eine Access-Datenbank (MS Office) erstellt worden (Anhang 9). Sie genügen den Erfordernissen dieser Arbeit. Sie können, ohne die eingegebenen Inhalte zu verändern, den Bedürfnissen anderer Bearbeiter in ergonomischer, aber auch in erläuternder Hinsicht angepasst werden. Ferner sind sie für Angaben, die sich im Laufe weiterer, auf dieser Arbeit aufbauender Forschungsaktivitäten ergeben, erweiterbar.

5 Anwendung

Im Abschnitt 5.1 wird das im vorhergehenden Kapitel entwickelte Vorgehen zum Definieren einer generischen Referenz am Beispiel eines Teilbereichs der Betriebsverfahren angewendet. Das Beispiel geht auf ein Projekt zurück, das im Auftrag und unter Beteiligung von Experten der Deutschen Bahn AG durchgeführt worden ist. Die dabei gemachten Erfahrungen werden begleitend dargelegt. Darüber hinaus wird im Abschnitt 5.2 die prinzipielle Anwendbarkeit des Vorgehens zur Analyse bereits definierter Funktionen gezeigt. Die bei der Anwendung gewonnenen Erkenntnisse und Erfahrungen werden im Abschnitt 5.3 zusammengefasst.

5.1 Definitionsbeispiele

Die im Kapitel 4 vorgestellten Ansätze werden am Beispiel eines Teilbereichs der Betriebsverfahren angewendet, der der Bereitstellung und Sicherung von Fahrwegen dient. Dieser Teilbereich darf nicht nur als Kern der Betriebsverfahren betrachtet werden, sondern er hat wegen der vielfältigen Möglichkeiten, Mensch und Technik zu kombinieren, eine besonders große Vielfalt an Systemarchitekturen hervorgebracht. Es darf davon ausgegangen werden, dass wegen dieser heterogenen Ausgangssituation nicht nur das Definieren generischer Funktionen von besonderem Interesse ist, sondern dass es wegen der spezifischen Realisierungen auch hohe Anforderungen hinsichtlich des Abstraktionsvermögens der zu beteiligenden Fachleute erfordert.

Der Autor dieser Arbeit konnte in einem für die Deutsche Bahn AG bearbeiteten Projekt[32] die vorgestellten Ansätze zur generischen Definition betrieblicher Grundfunktionen bereits während ihrer Entwicklung anwenden. So konnten die dabei im Kreise der beteiligten Fachleute gemachten Erfahrungen mit in die Entwicklung einfließen und die Ergebnisse abgesichert werden.

Ein dem betreffenden Projekt übergeordnetes Ziel galt und gilt der Reduzierung der über die gesamte Lebensdauer von Stellwerken anfallenden Kosten[33]. Diese werden auch durch die Aufteilung der entsprechenden Funktionsrealisierungen zwischen Mensch und Technik beeinflusst. Um die Funktionsrealisierungen entsprechend der in den jeweiligen Einsatzgebieten vorliegenden betrieblichen Randbedingungen optimal aufzuteilen, waren in dem

[32] Projekt „Betriebliches Anforderungsmanagement“ (BAM) im Auftrag Deutsche Bahn AG, Systemverbund Bahn, Produktentwicklung und Systembetreuung LST, TET 2, Völckerstraße 5, 80939 München, Laufzeit 11/2007 – 12/2009

[33] „Die Entwicklung von Lösungsansätzen zur Reduzierung der Lebenszykluskosten elektronischer Stellwerke ist zentrales Ziel des Verbundvorhabens NeuPro Plus“. B. Elsweiler in „Schienenverkehr – sicher, leise, effizient“, herausgegeben vom Bundesministerium für Wirtschaft und Technologie, Referat Öffentlichkeitsarbeit, Berlin 9/2008

Projekt die Funktionen unabhängig von den erst später festzulegenden Aufteilungen zu definieren. Dazu war das Denken in den Kategorien „Leit- und Sicherungstechnik“ und „Regelwerk“ zu vermeiden und die Funktionen folglich in einem übergeordneten Sinne als betriebliche Grundfunktionen zu definieren. Um die Fokussierung auf bekannte technische Lösungen zu vermeiden, wurden von Beginn an nicht nur mit dem CENELEC-Prozess erfahrene LST-Experten, sondern in gleichem Umfang auch Regelwerksexperten in die Projektarbeiten einbezogen.

Unter Beteiligung der Fachleute wurden in mehreren Workshops die Grenzen des zu definierenden funktionalen Systems festgelegt. Darauf aufbauend wurden die in ihm enthaltenen betrieblichen Funktionen top-down definiert und mit den Experten abgestimmt. Die im Abschnitt 5.1.1 folgende Definition des funktionalen Systems, die in dem Abschnitt 5.1.2 abgeleiteten Funktionsgruppen und die unter 5.1.3 als Beispielanwendung erläuterten Funktionen basieren inhaltlich auf den Arbeitsergebnissen des Projekts „Betriebliches Anforderungsmanagement“. Sie berücksichtigen jedoch die gemachten Erfahrungen durch ein strengeres formales Vorgehen.[34] Dies gilt insbesondere für die ausschließlich zweckorientierte Definition der Funktionen und ihre Abgrenzung gegenüber anderen Funktionen.

5.1.1 Funktionales System

Das im Anwendungsbeispiel betrachtete funktionale System umfasst einen dem Betreiben der Infrastruktur zuzurechnenden Teilbereich der Betriebsverfahren. Dieser lässt sich funktional als ein betrieblicher Prozess „Fahrten verschiedener Fahrzeuge zum Transport von Personen und Gütern auf der Infrastruktur eines Verkehrsnetzes sicher lenken und fahren“ umreißen. Innerhalb dieses Prozesses kann im Hinblick auf die angestrebte funktionale Differenzierung zwischen „Geeignete Fahrwege für das Durchführen von Fahrten sichern und freigeben“ und „Fahrzeuge fahren“ unterschieden werden. Ersteres deckt den mit dem nachfolgend behandelten Beispiel angestrebten Betrachtungsraum ab. Der Fokus ist folglich auf ein System ausschließlich realisierungsunabhängig zu definierender Funktionen zum Sichern und Freigeben von Fahrwegen zur Durchführung von Fahrten[35] gerichtet,

[34] Das strengere formale Vorgehen erlaubt zudem, wie bereits im Abschnitt 4.5 erwähnt, eine datenbankgestützte Aufbereitung der Definitionen und der mit ihnen im Zusammenhang stehenden weiteren Informationen, wie z.B. abgeleitete Gefährdungen und Realisierungsbeispiele.

[35] In der Beispielanwendung wird nicht das Fahren und Steuern des Fahrzeugs Gegenstand der Betrachtung sein. Gleiches gilt für die Funktionen von Prozessen, die den Betriebsablauf dispositiv beeinflussen oder der Information von Kunden, z.B. durch eine Wagenlaufverfolgung, dienen. Sie sollten, da die Funktionen generisch, d.h. unabhängig von Architekturen, definiert werden sollen, im Sinne eines Zwiebelschalenmodells zu einem späteren Zeitpunkt ergänzt werden können.

die durch unterschiedliche Kombinationen *betrieblicher Regeln und technischer Mittel*[36] realisiert werden können.

5.1.1.1 Funktionale Systemumgebung

Die zunächst vage wirkende Formulierung des zu betrachtenden Prozesses „Geeignete Fahrwege für das Durchführen von Fahrten sichern und freigeben“ wird entsprechend 4.1.2 durch die Beschreibung seiner funktionalen Umgebung präzisiert. Dazu werden Terminatoren angegeben, die mit dem betrachteten Prozess in Verbindung stehen. Im Bild 38 werden das zu definierende funktionale System, seine Terminatoren und die zwischen ihnen bestehenden Informationen in einer der *Strukturierten Analyse*, vgl. a. [DEM79], entlehnten Darstellungsform, einem Kontext-Diagramm, dargestellt. Im Hinblick auf eine konsequent architektur- und realisierungsunabhängige Systemdefinition sind auch die Terminatoren nach Möglichkeit als Prozesse und nicht als konkrete Systeme beschrieben worden. Die Terminatoren und das zu definierende betriebliche System werden im Abschnitt 5.1.1.2 durch die Betrachtung der zwischen ihnen bestehenden grundlegenden Informationsflüsse konkretisiert und gegeneinander abgegrenzt. Betrachtet werden nur primäre Informationsflüsse. Dies sind die grundlegenden Informationsflüsse, ohne die eine Beziehung zwischen dem zu betrachtenden Prozess und einem Terminator generell nicht beschreibbar wäre. Informationsrückflüsse sind u.U. nur bei bestimmten Realisierungen erforderlich. Sie können deshalb nicht als generisch gelten und werden weder zur Abgrenzung herangezogen noch im Kontext-Diagramm dargestellt.

[36] Diese Formulierung orientiert sich an der Definition von PACHL, nach der ein Betriebsverfahren ein „System betrieblicher Regeln und technischer Mittel zur Durchführung von Fahrten mit Eisenbahnfahrzeugen auf einer Eisenbahninfrastruktur“ ist [PAC08].

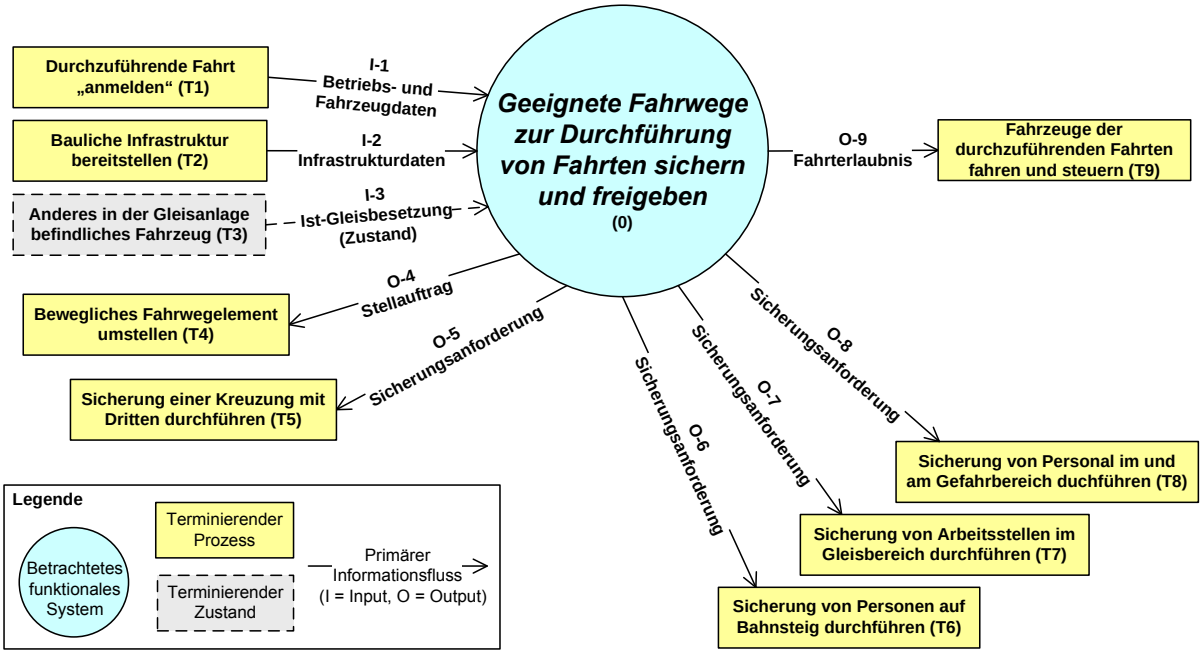


Bild 38: Kontext-Diagramm als Ausgangpunkt der generischen Systemdefinition

Erfahrungen

Die Beschreibung des zu betrachtenden funktionalen Systems und der mit ihm in Beziehung stehenden Umgebung hat sich auch bei einer streng generischen Betrachtungsweise als praktikabel erwiesen. Weil die Grenzen eines generisch definierten funktionalen Systems im Gegensatz zu einer festgelegten Abgrenzung, z.B. zwischen einer Stellwerksinnen- und einer Stellwerksaußenanlage, nur schwer erfassbar sind und deshalb als wenig konkret erscheinen, hat sich die Abgrenzung des zu definierenden funktionalen Bereichs durch die Angabe von Terminatoren als hilfreich erwiesen, um allen Beteiligten einen Orientierungsrahmen zu geben. Die grafische Darstellungsform erlaubte zudem einen guten Überblick über die Elemente der Umgebung des zu betrachtenden Systems. Das grundsätzliche Problem einer jeden Systemdefinition, das Führen eines Nachweises der Vollständigkeit, bleibt aber auch bei dieser Vorgehensweise erhalten. Ihm kann jedoch durch die transparente Darstellungsform und die Einbeziehung von Experten begegnet werden. Das Fehlen jeglicher innerer Systemarchitekturen lässt ein unkompliziertes Nachführen der entsprechenden Terminatoren und Inputs bzw. Outputs erwarten. Für sie kann anhand des von ihnen ausgehenden Inputs geprüft werden, ob sie tatsächlich „vergessen“ worden sind oder bereits in einer der definierten Funktionen als Teilfunktion enthalten sind.

5.1.1.2 Abgrenzung des funktionalen Systems

Das im Bild 38 dargestellte Kontext-Diagramm gibt bereits einen ersten Überblick über das zu definierende funktionale System und seine Umgebung. In der Tabelle 23 werden die abgebildeten terminierenden Prozesse und Zustände sowie die von ihnen ausgehenden

prinzipiellen Inputs und die vom betrachteten System zu erbringenden Outputs beschrieben. Der Zuschnitt der Terminatoren und insbesondere ihre Bezeichnung sind für die Definition des funktionalen Systems von untergeordneter Bedeutung. Vielmehr ist im Rahmen der generischen Sichtweise entscheidend, was dem zu definierenden System als Input zur Verfügung steht, um den von ihm erwarteten Output zu erzeugen.

Die Aufgabe der späteren Funktionsträger des zu definierenden funktionalen Systems besteht darin, die zur Verfügung stehenden Inputs so miteinander zu verknüpfen, dass der erwartete Output als Wert ausgegeben bzw. als Zustand erzeugt werden kann. Hieraus lassen sich die Aufgaben ableiten, die das System dazu erfüllen muss. Sie werden in der dritten Spalte der Tabelle 23 beschrieben und im Abschnitt 5.1.2 als Funktionsgruppen definiert.

Tabelle 23: Abgrenzung

Terminierender Prozess / Zustand	Abgrenzung u.a. durch Angaben zum In- und Output	Abgeleitete Aufgaben des zu definierenden funktionalen Systems
Durchzuführende Fahrt „anmelden“ (T1) Das Sichern und Freigeben eines geeigneten Fahrwegs ist eine Voraussetzung, um eine Fahrt durchführen zu können. Die Fahrtabsicht muss beim zu definierenden funktionalen System im weitesten Sinne des Wortes „angemeldet“ werden. Die Initialisierung findet in der Anforderung eines Fahrwegs ihren Ausdruck. Dazu müssen dem zu definierenden funktionalen System spätestens mit der Fahrweganforderung auch die Betriebs- und Fahrzeugdaten übergeben worden sein, die für die sichere Durchführung der Fahrt benötigt werden.	Es werden abfahrfertige Fahrzeuge betrachtet, bei denen die Be-/Entladung oder das Ein-/Aussteigen abgeschlossen sind. Die Eigenschaften der Fahrzeuge sind bereits ermittelt worden und werden dem zu definierenden funktionalen System zur Verfügung gestellt. Die Betriebsdaten der durchzuführenden Fahrt, z.B. Start-Ziel-Kombination, Zwischenpunkte und Haltezeiten, werden ebenfalls zur Verfügung gestellt.	Die betrieblichen und fahrzeugtechnischen Anforderungen sind mit der verfügbaren baulichen Infrastruktur in Einklang zu bringen, bevor eine Fahrt eines Fahrzeugs stattfinden darf. Es ergeben sich folgende Aufgaben: - Bilden einer geschlossenen Kette von Fahrwegelementen zwischen Start- und Zielpunkt entsprechend der Betriebsdaten; - Kompatibilität zwischen Fahrweg und Fahrzeug sicherstellen (Eignung der Fahrwegelemente für die durchzuführende Fahrt); - Befahren nicht geeigneter oder nicht verfügbarer Fahrwegelemente verhindern.
Bauliche Infrastruktur bereitstellen (T2) Die bauliche Infrastruktur eines Verkehrsnetzes trägt, führt und umgibt die Fahrzeuge. Sie kann ferner Elemente der Energieversorgung umfassen. Die Fahrbahn und die Grenze des lichten Raums sind Schnittstellen zwischen den Fahrzeugen und der baulichen Infrastruktur. Bauliche Infrastruktureinrichtungen unterliegen stets einem Verschleißprozess. Es ist daher unabdingbar, Arbeits- und Baustellen einzurichten; diese terminieren den betrachteten Prozess, weil die entsprechenden Infrastrukturelemente nicht für Fahrten zur Verfügung stehen.	Der Prozess T2 stellt die Elemente der Fahrweginfrastruktur entweder mit oder ohne Einschränkungen oder gar nicht zur Verfügung. Im betrachteten Prozess sind die entsprechenden Informationen als Eingangsgrößen zu beachten und weiterzuverarbeiten. Infrastruktureinrichtungen, die dazu dienen, Funktionen innerhalb des funktionalen Systems zu erfüllen, werden nicht zu T2 gerechnet, selbst wenn sie am Fahrweg realisiert werden sollten. Dies betrifft im Wesentlichen Einrichtungen streckenseitiger Realisierungen von Leit- und Sicherungstechnik.	

Terminierender Prozess / Zustand	Abgrenzung u.a. durch Angaben zum In- und Output	Abgeleitete Aufgaben des zu definierenden funktionalen Systems
Anderes in der Gleisanlage befindliches Fahrzeug (T3) Beim Terminator T3 handelt es sich nicht um einen Prozess. Der Terminator wird im Sinne eines physikalischen Grundzustandes „Fahrzeug auf Gleis“ verstanden. Dazu zählt ggf. auch die Inanspruchnahme des zu einem Gleis gehörenden lichten Raums durch ein Fahrzeug im Nachbargleis.	Der Terminator T3 besitzt und erzeugt keine Informationen. Als „Input“ liegt dem zu definierenden funktionalen System lediglich ein elementarer physikalischer Grundzustand „Fahrzeug auf Gleis“ vor. Er muss vom zu definierenden funktionalen System erst zu einer logischen und damit weiter verwertbaren Information aufbereitet werden.	- Erfassen physikalischer Grundzustände „Fahrzeug auf Gleis“ und Weiterverarbeitung zu einer logischen gleisbezogenen Besetzungsinformation, die den Ort*) der Besetzung angibt; - Prüfen der benötigten Fahrwegelemente einschließlich ihrer lichten Räume auf das Freisein von Fahrzeugen; - Erzeugen und Verwalten logischer Belegungsinformationen, die sich aus Fahrzeugbewegungen, z.B. als Vorbelegung, ergeben. *) Da Fahrzeuge eine Ausdehnung besitzen, wird Ort als ein Bereich mit Längenausdehnung verstanden.
Bewegliches Fahrwegelement umstellen (T4) Bewegliche Fahrwegelemente sind wesentliche Merkmale spurgeführter Verkehrssysteme. Sie müssen in Abhängigkeit von der Start-Ziel-Relation u.U. für jede Fahrt eine andere Stellung einnehmen. Das Umstellen ist ein mechanischer Vorgang, für den entsprechende Umstellkräfte aufgebracht werden müssen.	Die Fahrwegelemente und ihre Antriebe werden nicht zum betrachteten funktionalen System gezählt. Dagegen ist die logische Ansteuerung des Antriebs durch einen Stellbefehl Bestandteil des zu definierenden funktionalen Systems.	- Generieren und ausgeben von Steuerbefehlen an die beweglichen Fahrwegelemente; - Beibehalten der beabsichtigten Lage, solange die beweglichen Fahrwegelemente von einer Fahrt beansprucht werden.

Terminierender Prozess / Zustand	Abgrenzung u.a. durch Angaben zum In- und Output	Abgeleitete Aufgaben des zu definierenden funktionalen Systems
Sicherung einer *Kreuzung mit Dritten* durchführen (T5) Ebenso wie bewegliche Fahrwegelemente muss der Sicherungszustand einer Kreuzung mit Dritten in Abhängigkeit von einer Fahrt geändert werden. Der Terminator führt die Sicherung auf Anforderung durch.	Das Durchführen der Sicherung ist nicht Bestandteil des betrachteten funktionalen Systems. Dagegen ist ihre Auslösung Bestandteil des zu definierenden funktionalen Systems. Es gibt eine Sicherungsanforderung aus.	- Generieren und Ausgabe von Sicherungsanforderungen, mit denen die Sicherung der Kreuzungen mit Dritten so rechtzeitig angestoßen wird, dass die Kreuzung gesichert ist, bevor das Eisenbahnfahrzeug sie erreicht.
Sicherung von *Personen auf Bahnsteigen* durchführen (T6) Bahnsteige sind Schnittstellen zwischen den Fahrzeugen und den Reisendenzu- und –abgängen. Aufgrund ihrer Anordnung unmittelbar an den Gleisen überschneiden sie sich in einem Teilbereich mit dem Gefahrenbereich bewegter Fahrzeuge. Der Terminator führt im Falle von Fahrten im entsprechenden Gleis die Sicherung von Personen auf dem angrenzenden Bahnsteig durch.	Es geht nicht um das Ein- und Aussteigen, sondern um den Schutz von Reisenden, die sich am oder im Gefahrbereich bewegter Fahrzeuge aufhalten. Die Sicherung selbst ist nicht Bestandteil des betrachteten funktionalen Systems. Es gibt eine Sicherungsanforderung aus.	- Generieren und Ausgabe einer Sicherungsanforderung, mit der die Sicherung von Reisenden auf Bahnsteigen angestoßen wird.
Sicherung von *Arbeitsstellen im Gleis* durchführen (T7) Arbeitsstellen befinden sich im Gefahrenbereich des Fahrwegs. Sie sind zu sichern. Die Sicherung erfolgt durch das Fernhalten des Personals vom Gefahrbereich.	Das Durchführen der Sicherung ist nicht Bestandteil des betrachteten funktionalen Systems. Es gibt eine Sicherungsanforderung aus.	- Generieren und Ausgabe einer Sicherungsanforderung, mit der die Sicherung von Arbeitsstellen angestoßen wird.
Sicherung von *Personal in und an Fahrzeugen* durchführen (T8) Die Sicherung erfolgt durch das Fernhalten des Personals vom Gefahrbereich.	Das Durchführen der Sicherung ist nicht Bestandteil des betrachteten funktionalen Systems. Es gibt eine Sicherungsanforderung aus.	- Generieren und Ausgabe einer Sicherungsanforderung, mit der die Sicherung des Personals angestoßen wird.

Terminierender Prozess / Zustand	Abgrenzung u.a. durch Angaben zum In- und Output	Abgeleitete Aufgaben des zu definierenden funktionalen Systems
Fahrzeug der durchzuführenden Fahrt fahren und steuern (T9) Um Fahrzeuge entlang eines Fahrwegs auf bestimmte Geschwindigkeiten beschleunigen und abbremsen zu können, müssen Antriebs- und Bremskräfte bereitgestellt und gesteuert werden.	Das Fahrzeug selbst ist nicht Teil des betrachteten Prozesses. Dies gilt auch für das Erzeugen und Steuern der Antriebs- und Bremskräfte. Das Steuern des Fahrzeugs beginnt mit dem Empfang der vom betrachteten funktionalen System ausgegebenen Fahrbefehle.	- Freigabe eines geeigneten Fahrwegs; - Sichern des freigegebenen Fahrwegs für die Dauer der Beanspruchung durch die Fahrt.

Erfahrungen

Die Abgrenzung des zu definierenden funktionalen Systems hat den beteiligten Fachleuten, insbesondere jenen aus dem Bereich der Stellwerke, ein hohes Abstraktionsvermögen abverlangt, weil die Grenzen des zu definierenden Systems nicht zwangsläufig mit den Grenzen der ihnen im Rahmen der beruflichen Praxis geläufigen realisierten Einheiten, wie z.B. einer Stellwerksinnenanlage, übereinstimmen. Die von „außen nach innen“ erfolgte, d.h. mit der Beschreibung der Terminatoren beginnende Abgrenzung hat sich bei diesem Schritt als hilfreich erwiesen, weil mit der so geschaffenen „virtuellen“ Grenze Ersatz für die „gewohnten“, aber im Hinblick auf den generischen Ansatz zu vermeidenden Grenzen realisierter Einheiten geschaffen werden konnte. Das so abgegrenzte System wurde in dem Expertenkreis schließlich als ein fest definierter Rahmen aufgefasst, innerhalb dessen die Grenzen unterschiedlich realisierter Einheiten variabel sein können. So kann z.B. die Anforderung der Sicherung eines Bahnübergangs einer Stellwerksanlage entstammen, durch ein mündliches Verfahren zwischen Fahrdienstleiter und Schrankenwärter, einen Einschaltkontakt am Gleis oder eine Pfeiftafel ausgelöst werden.

Die in der Tabelle 23 enthaltenen Formulierungen und die abgeleiteten Aufgaben mögen selbstverständlich klingen. Dennoch wäre, ausgehend von jeder einzelnen Lösungsmöglichkeit, die im vorstehenden Absatz beispielhaft genannte Funktionalität von Fachleuten unter dem Blickwinkel und dem Sprachgebrauch einer konkreten Realisierung entsprechend unterschiedlich beschrieben worden, wie z.B. „Auftrag zum Schließen an Schrankenwärter erteilen“ oder „Annäherung eines Eisenbahnfahrzeugs ankündigen“ für die Pfeiftafel. Wobei die Pfeiftafel bei exakter Betrachtung nur den Auftrag zum Pfeifen erteilt und das Pfeifen selbst erst dem mit dem Senken der Schrankenbäume funktional vergleichbaren Sicherungsvorgang gleichkommt.

Es hat sich gezeigt, dass die realisierungsunabhängigen Formulierungen nicht nur eine zweite, u.U. auch kontrollierende Sichtweise auf bestimmte Funktionsrealisierungen erlauben, sondern im Sinne einer generischen Referenz auch zu deren funktionaler Vergleichbarkeit beitragen können. Zugleich hat das realisierungsunabhängige Definieren einschließlich jenes der Terminatoren bereits auf dieser Betrachtungsebene zu neutralen Formulierungen dessen geführt, was innerhalb des zu definierenden funktionalen Systems als Aufgaben auszuführen ist.

5.1.2 Betriebliche Funktionsgruppen

Die in der Tabelle 23 identifizierten und von dem zu definierenden funktionalen System zu leistenden Aufgaben wurden zu Funktionsgruppen zusammengefasst, die, den zu definierenden Funktionen übergeordnet, als Gliederung einer hierarchisch aufgebauten Funktionsliste herangezogen werden sollen. Im Einzelnen handelt es sich um die im Bild 39 eingetragenen fünf Funktionsgruppen.

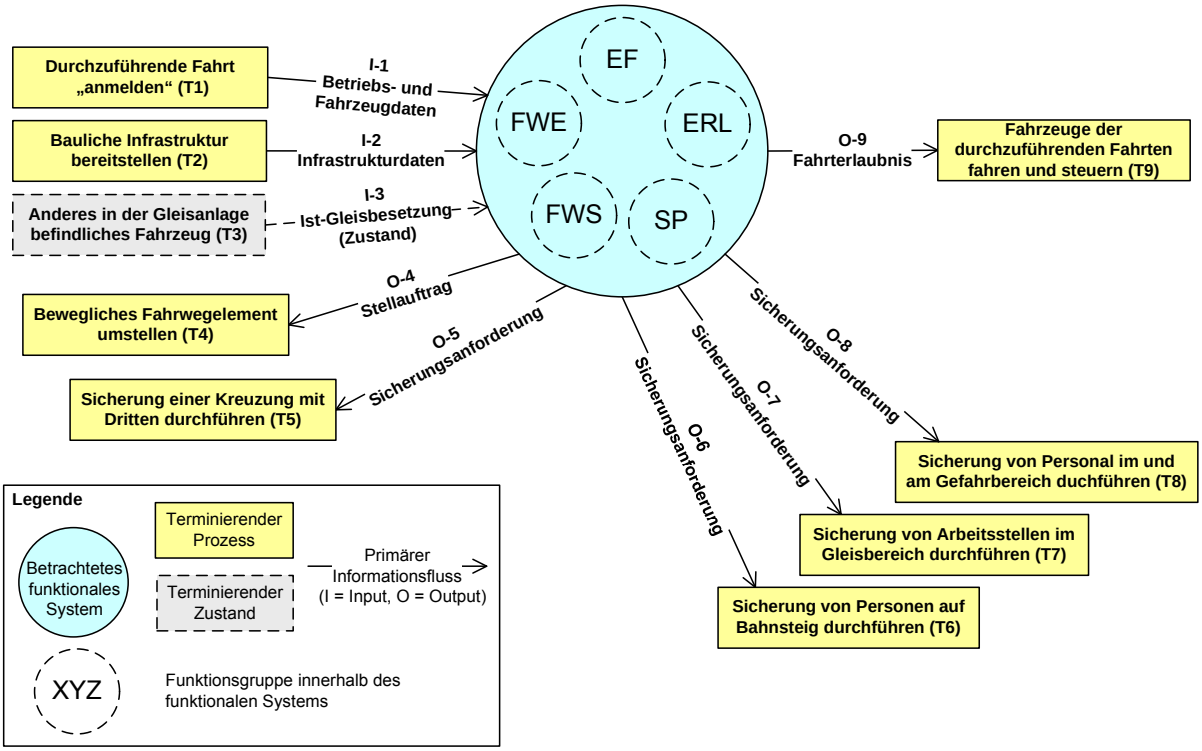


Bild 39: Identifizierte Funktionsgruppen im Kontext mit den Terminatoren[37]

Im Einzelnen bedeuten:

EF Ermitteln der zur Start-Ziel-Kombination gehörenden Fahrwegelemente,

FWE Fahrweg auf Eignung prüfen „Fahrwegeignung“,

FWS Fahrweg auf Freisein prüfen, einstellen und sichern „Fahrwegsicherung“,

ERL Fahrterlaubnis und Restriktionen erteilen,

SP Sichern von Personen/-gruppen, die durch die Fahrt gefährdet werden können.

Bereits die Funktionsgruppen können wie Funktionen durch die Angabe ihres Zwecks definiert werden. Die Tabelle 24 enthält dazu die Spalte mit der Formulierung „Ausführung, um …“. Sie gibt den Zweck einer jeden Funktionsgruppe wieder und ist als Kern ihrer generischen Definition zu betrachten. Die Namen der Funktionsgruppen können deshalb gegenüber den vorstehenden Formulierungen zu kürzeren, prägnanteren Begriffen „gestrafft“ werden.

[37] Die identifizierten Funktionsgruppen werden hier in Anlehnung an das Kontext-Diagramm der Strukturierten Analyse dargestellt. Die Abbildung der nächsten Gliederungsstufe innerhalb eines „Bubbels“ ist an sich nicht üblich. Sie wird hier aber aus Gründen der Anschauung gewählt, um die Beziehung zwischen den außenliegenden Terminatoren und den innerhalb des zu betrachtenden Systems liegenden Funktionsgruppen zu zeigen.

Tabelle 24: Funktionsgruppen des zu definierenden funktionalen Systems

Name		Ausführung um …	Erläuterung
EF	Fahrwegermittlung	… einen zwischen einem Start- und einem Zielpunkt liegenden Fahrweg zu ermitteln.	Der von einem Start- zu einem Zielpunkt führende Fahrweg muss bekannt sein.
FWE	Fahrwegeignungs-prüfung	… die Eignung des Fahrwegs einschließlich seiner Betriebsbereitschaft für ein Fahrzeug / einen Fahrzeugverband festzu-stellen.	Der Fahrweg muss für das Fahrzeug / den Fahrzeugverband und das Durchführen der Fahrt geeignet und betriebsbereit sein.
FWS	Fahrwegsicherung	… einen freien Fahrweg einzustellen und gegenüber anderen Fahrzeugen / Fahrzeugverbänden sowie querenden Dritten zu sichern.	Die zwischen einem Start- und einem Zielpunkt liegenden Fahrwegelemente müssen frei von anderen Beanspru-chungen sein. Die beweglichen Fahrwegelemente müssen sich in der erforderlichen Lage befinden und der Fahrweg gegen kreuzende Dritte gesichert sein.
ERL	Fahrterlaubnis und Restriktionen	… eine Fahrt vom Start- zum Zielpunkt unter Vorgabe der erforderlichen Restriktionen zuzulassen.	Sofern alle Voraussetzungen für eine Fahrt vorliegen, kann die Fahrt freigegeben werden. Zu den Voraus-setzungen können Restriktionen, wie z.B. Geschwindigkeitsvorgaben gehören, die der Fahrt ebenfalls vorzugeben sind.
SP	Sicherung von Personen	… Personen zu sichern, die außerhalb des Fahrzeugs durch das bewegte Fahrzeug gefährdet werden können.	Personen können berechtigt sein, an einem stehenden Eisenbahnfahrzeug oder in einem Gleisbereich Tätigkeiten auszuführen; ferner können sich Personen auf Bahnsteigen in Bereichen aufhalten, die sich mit dem Gefahrenraum bewegter Fahrzeuge überschneiden.

Erfahrungen

Die Funktionsgruppen strukturieren das zu definierende funktionale System. Sie besitzen damit eine den in komplexen realen Systemen enthaltenen Subsystemen vergleichbare Rolle: Sowohl die Bezüge zur Funktionalität des betrachteten funktionalen Systems und zu dem mit ihm verbundenen Betriebsprozess sind erkennbar als auch das dazu erforderliche prinzipielle Zusammenwirken der Funktionsgruppen. Die Zwecke sind dementsprechend unterschiedlichen Inhalts, sie überschneiden sich nicht. Mit der erfolgten Abgrenzung des zu definierenden Systems durch Terminatoren und dem Festlegen der Funktionsgruppen ist

das funktionale System im Kreise der beteiligten Fachleute auch ohne Bezüge zu existierenden technischen Lösungen als ein fest umrissener Bereich aufgefasst worden, innerhalb dessen Funktionen wie für konkrete Subsysteme definiert werden können.

Die für die Funktionsgruppen formulierten Zwecke sind, wenn auch in unterschiedlicher Intensität, durch Aufzählungen geprägt. Dies wird anhand von Formulierungen wie z.B. „und", „unter Vorgabe" oder „einschließlich" deutlich. Es können offenbar auf dieser hohen Betrachtungsebene keine Alternativen ausschließenden Zweckformulierungen gefunden werden. Vielmehr wird die Notwendigkeit zur weiteren funktionalen Untergliederung einer jeden Funktionsgruppe unterstrichen.

5.1.3 Betriebliche Grund- und Teilfunktionen

Die Verwendung der im Abschnitt 4.5 vorgestellten Datenbankformulare zum Definieren von Funktionen und zum Identifizieren ihrer gefährlichen Ergebnisse wird nachfolgend am Beispiel eines mehrstufigen Pfades[38] der Funktionsgruppe „Fahrwegsicherung" erläutert. Dazu werden die entsprechend der Formularfelder zu tätigenden Eingaben angegeben und erläutert.

5.1.3.1 Struktur der zu definierenden Funktionsgruppe

Das Definieren der Grundfunktionen setzt die Strukturierung der entsprechenden Funktionsgruppe voraus. Umgekehrt wird aber auch zur Strukturierung zumindest eine Vorstellung vom dem gebraucht, was mit den Funktionen und Teilfunktionen bezweckt wird. Deshalb sind die hierarchische Gliederung der Funktionsgruppe und das Definieren ihrer Funktionen bzw. Teilfunktionen in einem iterativen Abstimmungsprozess mit den beteiligten Fachleuten der DB AG erfolgt, der im Einzelnen an dieser Stelle nicht weiter erörtert wird. Sofern erforderlich, wird bei der Erläuterung der im Formular zu tätigenden Eingaben darauf eingegangen. Im Kontext mit den anderen Funktionsgruppen ist die Funktionsgruppe „Fahrwegsicherung", wie im Bild 40 dargestellt, strukturiert worden[39]. Weitergehende Erläuterungen zur Struktur enthält der Anhang 6.

[38] Die Gliederung einer Funktionsgruppe in Funktionen und deren Teilfunktionen führt i.d.R. zu einem hierarchischen Aufbau, der mehrere Pfade enthält, die ausgehend von der Funktionsgruppe über eine oder mehrere Gliederungsstufen zu den einzelnen Teilfunktionen führen.

[39] Im Bild 40 werden aus Gründen der Übersichtlichkeit nur die Funktionsnamen angegeben. Die Definitionen und ggf. weitere Erläuterungen sind in der Funktionsliste enthalten (Anhang 5).

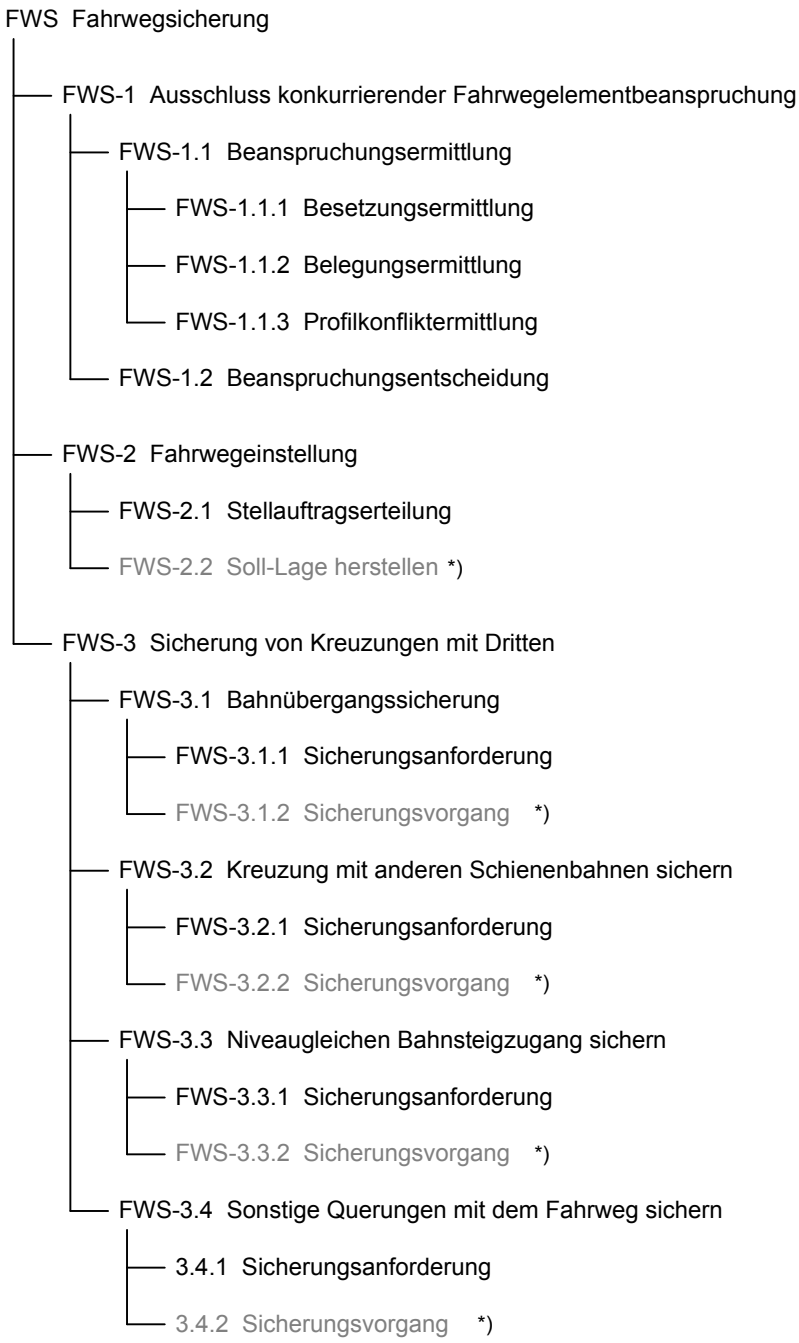


Bild 40: Struktur der Funktionsgruppe „Fahrwegsicherung“[40]

[40] Die mit „*)“ markierten Teilfunktionen gehören nach der im Abschnitt 5.1.1.2 vorgenommen Abgrenzung nicht zum betrachteten funktionalen System (Bild 38, Bild 39), sondern sind den Terminatoren zuzurechnen. Das so abgegrenzte funktionale System gilt folglich erst ab einer entsprechenden Betrachtungsebene. Darüber sind die Terminatoren Bestandteile übergeordneter funktionaler Systeme, deren Zwecke jedoch identisch mit denen der jeweiligen Terminatoren sind.

5.1.3.2 Eingabebeispiele

Am Beispiel eines Auszugs aus der Funktionsgruppe FWS „Fahrwegsicherung“ werden die zur Definition einer Funktion und zur Identifizierung ihrer gefährlichen Ergebnisse in den Eingabemasken zu tätigenden Eingaben vorgestellt. Betrachtet werden drei aufeinander aufbauende, aber in unterschiedlichen Ebenen liegende Funktionen. Aus Abbildungs- und Platzgründen werden die Eintragungen nicht in den Eingabemasken, sondern in den Tabelle 25 bis Tabelle 27 wiedergegeben, die jene Eingabefelder enthalten, in die Eintragungen vorgenommen worden sind. Im Anschluss an jede Tabelle folgen ergänzende Erläuterungen, die auch Erfahrungen wiedergeben.

Eingabebeispiel 1

Tabelle 25: Eingabebeispiel 1

Feld	**Eingetragener Feldinhalt**
Nummer	*FWS*
Funktionsname	*Fahrwegsicherung*
1 Definition betrieblicher Funktionen / Analyse definierter Funktionen	
Ausführung, um	*… einen freien Fahrweg einzustellen und gegenüber anderen Fahrzeugen / Fahrzeugverbänden sowie querenden Dritten zu sichern.*
Ergänzende Erläuterung	*Die zwischen einem Start- und einem Zielpunkt liegenden Fahrwegelemente müssen frei von anderen Beanspruchungen sein, d.h. andere Beanspruchungen ausgeschlossen sein (FWS-1). Die beweglichen Fahrwegelemente müssen sich in der erforderlichen Lage befinden (FWS-2) und der Fahrweg gegen kreuzende Dritte gesichert sein (FWS-3).*
OUTPUT und planmäßige Folgen	
Bezwecktes Ergebnis	*Gesicherter Fahrweg*
Zul. Ergebniswert 1	*„Fahrweg ist gesichert“*
Zul. Betriebl. Folgen 1	*→ Fahrt*
Erforderlicher INPUT	
Input 1	*s. zugeordnete Funktionen*
Einordnung	
Bezug zum Betriebsprozess	*Ein gesicherter Fahrweg ist unmittelbare Voraussetzung für das Fahren von Fahrzeugen. Der Bezug zum Betriebsprozess ist unmittelbar erkennbar.*
Klassifizierung als	*Funktionsgruppe (Fgr)*
Anmerkungen / Bemerkungen	*Auf dieser Betrachtungsebene nur sehr unspezifisch zu beschreiben → Behandlung als Funktionsgruppe → keine Angabe von Ergebniswerten und Input → keine Gefährdungsidentifikation*

Erläuterungen zum Eingabebeispiel 1

Der Kern der Definition umfasst Angaben zum Zweck der Funktion („Ausführung, um …“) sowie die Vergabe einer Nummer und eines Funktionsnamens. Als sehr kurze Definition wäre „Ausführung, um einen gesicherten Fahrweg zu erhalten“ vorstellbar. Dabei bliebe jedoch offen, was einen gesicherten Fahrweg kennzeichnen soll. Deshalb wird eine Formulierung gewählt, die eine Aufzählung mehrerer Ziele umfasst. Aus diesem Grunde wird „Fahrwegsicherung“ nicht als Funktion, sondern als Funktionsgruppe eingestuft. Als Nummer wird eine sinnfällige Abkürzung des Namens der Funktionsgruppe gewählt. Die in der Definition enthaltenen Angaben werden mit einer Erläuterung ergänzt. Diese optionalen Angaben haben insbesondere die Arbeit mit der Eingabemaske unterstützt, weil mit ihnen inhaltlich auch auf die untergeordneten, noch zu definierenden Funktionen eingegangen werden kann. In der als eine Ergebnisform anzusehenden hierarchisch aufgebauten Funktionsliste (Anhang 5) ergeben sich derartige Verweise automatisch durch die unmittelbare Nähe der Zeilen der untergeordneten Funktionen (vgl. Anhang 5). Das Ergebnis dieser Funktionsgruppe ist ein „gesicherter Fahrweg“. Es wird zugleich als zulässiger Ergebniswert betrachtet, auf welchen als betriebliche Folge eine Fahrt erfolgen darf. Im Prinzip ist dieses Ergebnis in seiner Aussage sehr pauschal und bedarf, wie es in der Zweckbeschreibung geschehen ist, einer Differenzierung. Dies geschieht in der folgenden Ebene durch die in der Funktionsgruppe enthaltenen Funktionen. Da auf deren Ebene auch die gefährlichen Ergebnisse differenzierter angegeben werden können, wird auf Ebene der Funktionsgruppe keine Ergebnis-FMEA durchgeführt. Bezüglich des Inputs für die Funktionsgruppe wird auf die zugeordneten Funktionen, ggf. auf deren Teilfunktionen verwiesen, da er sich aus deren Inputs zusammensetzt und dort auf Basis der kleineren funktionalen Einheiten einfacher beschrieben werden kann. Ggf. kann im Rahmen einer Bottom-up-Betrachtung ein zusammenfassender Oberbegriff gefunden werden, der den hier gewählten Verweis ersetzen kann.

Eingabebeispiel 2

Das zweite Eingabespiel gilt der der Funktionsgruppe „Fahrwegsicherung“ zugeordneten betrieblichen Grundfunktion „Ausschluss konkurrierender Fahrwegelementbeanspruchungen“.

Tabelle 26: Eingabebeispiel 2

Feld	**Eingetragener Feldinhalt**
Nummer	*FWS-1*
Funktionsname	*Ausschluss konkurrierender Fahrwegelementbeanspruchung*
Definition	
Ausführung, um	*… untereinander unverträgliche Beanspruchungen von Fahrwegelementen durch Fahrzeuge oder Fahrzeugverbände auszuschließen.*

Feld	Eingetragener Feldinhalt
Nummer	*FWS-1*
Funktionsname	*Ausschluss konkurrierender Fahrwegelementbeanspruchung*
Ergänzende Erläuterung	*Der Ausschluss konkurrierender Beanspruchungen beruht auf einer Entscheidung über die Zulässigkeit beabsichtigter Beanspruchungen und dem Befolgen der Entscheidung. Ein Fahrwegelement darf nur zur Beanspruchung freigegeben werden, wenn es frei von anderen Beanspruchungen ist. Dazu müssen alle Formen der Fahrwegelementbeanspruchung ermittelt (FWS-1.1) sowie über die Zulassung einer neuen Beanspruchung entschieden werden (FWS-1.2).*
OUTPUT und planmäßige Folgen	
Bezwecktes Ergebnis	*Ausschluss konkurrierender Fahrwegelementbeanspruchung*
Zul. Ergebniswert 1	*„konkurrierende Beanspruchung ist ausgeschlossen“*
Zul. Betriebl. Folgen 1	*→ Fahrt*
Erforderlicher INPUT	
Input 1	*Summe des Inputs der zugeordneten Teilfunktionen*
Einordnung	
Bezug zum Betriebsprozess	*Da sich Fahrzeuge nicht durchdringen können, ist der Ausschluss konkurrierender Fahrwegbeanspruchungen eine unmittelbare Voraussetzung für das Fahren von Fahrzeugen. Der Bezug zum Betriebsprozess ist unmittelbar erkennbar.*
Klassifizierung als	*Betriebliche Funktion (BGrF)*
Anmerkungen / Bemerkungen	--
Identifizierung betrieblich gefährlicher Ergebnisse	
Nicht bezwecktes Ergebnis 1	*„Konkurrierende Beanspruchung ist nicht ausgeschlossen“*
Nicht bezwecktes Ergebnis 2	*„Nicht konkurrierende Beanspruchung ist ausgeschlossen“*
Ergebnis-FMEA	
Formulierung des falschen Ergebnisses 1	*Eine konkurrierende Beanspruchung ist nicht ausgeschlossen.*
Ablauf / Folgen 1	*Mehrere Unfallarten möglich: z.B. Entgleisungen wg. Umstellen von Fahrwegelementen vor/unter einem anderen Zug; Kollisionen mit Fahrzeugen im eigenen Gleis oder bei Fahrten in das Nachbargleis*
Einstufung 1	*Gefährliches Ergebnis*
Formulierung des falschen Ergebnisses 2	*Eine Beanspruchung ist ausgeschlossen, obwohl sie nicht in Konkurrenz steht.*
Ablauf / Folgen 2	*Eine zulässige Fahrt wird nicht durchgeführt.*
Einstufung 2	*Hemmung*

Erläuterungen zum Eingabebeispiel 2

Die definierte Funktion liegt auf der ersten Gliederungsstufe der Funktionsgruppe Fahrwegsicherung. Dementsprechend wird deren Abkürzung um eine Ziffer zu FWS-1 ergänzt. Gemäß Bild 40 soll sie dem Ausschluss konkurrierender Fahrwegelementbeanspruchungen dienen (vgl. a. Anhang 6). Dieser Zweck wird als in Verbindung mit „Ausführung, um …“ als Finalsatz formuliert. In der optionalen ergänzenden Erläuterung wird auf die auch bei generischer Betrachtung erkennbaren Teilfunktionen hingewiesen. Wie schon bei der übergeordneten Funktionsgruppe ergeben sich in der später hierarchisch aufgebauten Funktionsliste (Anhang 5) solche Verweise automatisch durch die unmittelbare Nähe der Zeilen der untergeordneten Funktionen. Das Ergebnis dieser Grundfunktion ist der erfolgreiche Ausschluss konkurrierender Fahrwegelementbeanspruchungen, als Ergebniswert wird „konkurrierende Beanspruchung ist ausgeschlossen“ formuliert. Auf dieses Ergebnis hin darf als betriebliche Folge eine Fahrt stattfinden. Der Bezug des Ausschlusses konkurrierender Fahrwegelementbeanspruchungen zum Betriebsprozess ist unmittelbar erkennbar. Im Gegensatz zur übergeordneten Funktionsgruppe, die mehrere Zwecke erkennen lässt, ist der Ausschluss konkurrierender Fahrwegelementnutzungen wesentlich enger gefasst und kann als ein Zweck aufgefasst werden. Die Funktion wird deshalb als betriebliche Grundfunktion (BGrF) eingestuft, zu der mehrere Teilfunktionen definiert werden können.

Zu Beginn der Ergebnis-FMEA sind bezogen auf das angestrebte Ergebnis nicht die bezweckten Ergebnisse zu bestimmen. Sie können aus dem bezweckten Ergebnis „konkurrierende Beanspruchung ist ausgeschlossen“ durch Negation abgeleitet werden. Dies führt zu zwei nicht bezweckten Ergebnissen: „Eine konkurrierende Beanspruchung ist nicht ausgeschlossen“ und „Eine Beanspruchung ist ausgeschlossen, obwohl sie nicht in Konkurrenz steht“. Die Folgenbetrachtungen zeigen, dass ersteres Ergebnis gefährlich und zweiteres sich hemmend auf den Betrieb auswirkt.

Hinweis: Nicht bezweckte Ergebnisse im Sinne von „Kein Ergebnis“ werden gemäß der Ausführungen im Abschnitt 4.3.4.1 nicht betrachtet.

Eingabebeispiel 3

Im dritten Eingabespiel wird eine Funktion definiert, die einer für den Ausschluss konkurrierender Fahrwegelementbeanspruchungen notwendigen Teilaufgabe dient.

Tabelle 27: Eingabebeispiel 3

Feld	**Eingetragener Feldinhalt**
Nummer	*FWS-1.1*
Funktionsname	*Beanspruchungsermittlung*
Definition	
Ausführung, um	*… alle Formen der Beanspruchung von Fahrwegelementen durch andere Fahrzeuge / andere Fahrzeugverbände zu ermitteln.*

Feld	Eingetragener Feldinhalt
Nummer	*FWS-1.1*
Funktionsname	*Beanspruchungsermittlung*
Ergänzende Erläuterung	*Zum Ausschluss konkurrierender Fahrwege müssen alle Formen der Fahrwegbeanspruchung ermittelt werden. In Abhängigkeit davon, wo sich das nutzende Fahrzeug befindet, ergeben sich unterschiedliche Beanspruchungsformen: Fahrzeug auf dem Fahrwegelement (FWS-1.1.1), Fahrzeug in Annäherung an das Fahrwegelement (FWS-1.1.2), Inanspruchnahme benachbarter lichter Räume (FWS-1.1.3).*
OUTPUT und planmäßige Folgen	
Ergebnis	*Wert des Beanspruchungszustands*
Zul. Ergebniswert 1	*„Fahrwegelement ist nicht beansprucht“*
Planm. Folgen 1	*→ Fahrt*
Zul. Ergebniswert 2	*„Fahrwegelement ist beansprucht“*
Planm. Folgen 2	*→ Abweisung der beabsichtigten Beanspruchung*
Erforderlicher INPUT	
Input 1	*Summe des Inputs der zugeordneten Teilfunktionen*
Einordnung	
Bezug zum Betriebsprozess	*Der Bezug zum Betriebsprozess ergibt sich mittelbar über die übergeordnete Funktion FWS-1, die dem Ausschluss konkurrierender Beanspruchungen dient. FWS-1.1 wird deshalb als Betriebliche Teilfunktion eingestuft.*
Klassifizierung als	*Betriebliche Teilfunktion (BTf)*
Anmerkungen / Bemerkungen	--
Identifizierung betrieblich gefährlicher Ergebnisse	
Nicht bezwecktes Ergebnis 1	--
Ergebnis-FMEA	
Formulierung des falschen Ergebnisses 1	*Für ein Fahrwegelement wird keine Beanspruchung ermittelt, obwohl es beansprucht ist.*
Ablauf / Folgen 1	*Mehrere Unfallarten möglich: z.B. Entgleisungen wg. Umstellen von Fahrwegelementen vor/unter einem anderen Zug; Kollisionen mit Fahrzeugen im eigenen Gleis oder bei Fahrten in das Nachbargleis*
Einstufung 1	*Gefährliches Ergebnis*
Formulierung des falschen Ergebnisses 2	*Für ein Fahrwegelement wird eine Beanspruchung ermittelt, obwohl es nicht beansprucht ist.*
Ablauf / Folgen 2	*Eine zulässige Fahrt findet nicht statt.*
Einstufung 2	*Hemmung*

Erläuterungen zum Eingabebeispiel 3

Die definierte Funktion liegt auf der zweiten Gliederungsstufe der Funktionsgruppe Fahrwegsicherung. Dementsprechend wird deren Abkürzung zu FWS-1.1 ergänzt. Gemäß Bild 40 soll sie der Ermittlung von Fahrwegelementbeanspruchungen dienen (vgl. a. Anhang 6). Dieser Zweck wird wie bei den anderen Funktionen als in Verbindung mit „Ausführung, um …“ als Finalsatz formuliert. Wegen der drei, auch bei einer generischen Betrachtung, sehr unterschiedlichen Formen der Beanspruchung ergeben sich für die zu definierende Funktion drei entsprechende Teilfunktionen. Sie werden in der optionalen ergänzenden Erläuterung aufgeführt. Das Ergebnis der zu definierenden Funktion ist ein gültiger Wert des Beanspruchungszustands. Dies sind „Fahrwegelement ist nicht beansprucht“ und „Fahrwegelement ist beansprucht“. Auf das erste Ergebnis hin darf als betriebliche Folge eine Fahrt stattfinden. Im Fall des zweiten Ergebnisses muss eine beabsichtigte Beanspruchung abgewiesen werden. Der Bezug der Beanspruchungsermittlung zum Betriebsprozess ergibt sich über den Ausschluss konkurrierender Fahrwegelementbeanspruchungen, der als Betriebliche Grundfunktion definiert worden ist. Deshalb wird die Beanspruchungsermittlung als Betriebliche Teilfunktion (BTf) eingestuft, die einen Beitrag zu der übergeordneten Funktion liefert.

Für das bezweckte Funktionsergebnis sind zwei zulässige Werte festgelegt worden, die nur situativ wahr sind. Darüber hinaus lassen sich keine weiteren falschen Ergebniswerte ableiten, die als nicht bezweckte Ergebnisse einzutragen wären. Als gefährliches Ergebnis wird „Für ein Fahrwegelement wird keine Beanspruchung ermittelt, obwohl es beansprucht ist“ und als hemmendes Ergebnis „Für ein Fahrwegelement wird eine Beanspruchung ermittelt, obwohl es nicht beansprucht ist“ formuliert.

Hinweis: Nicht bezweckte Ergebnisse im Sinne von „Kein Ergebnis“ werden gemäß der Ausführungen im Abschnitt 4.3.4.1 nicht betrachtet.

5.1.3.3 Ergebnis-/Ausgabebeispiel „Funktionsliste“

Aus den über die Masken eingegebenen und in der Datenbank gespeicherten Daten können Ausgaben unterschiedlicher Detaillierungstiefe generiert werden. Tabelle 28 zeigt beispielhaft den Auszug aus einer Liste mit den Fahrwegsicherungsfunktionen, die aus den drei vorstehenden Eingabebeispielen abgeleitet worden ist. Die Liste ist in ihrer Struktur an jener der prEN 15380-4 orientiert; sie wird im Anhang 5 in ihrem gesamten Umfang wiedergegeben. Je nach Erfordernis des Anwenders kann der inhaltliche Umfang reduziert oder um zusätzlich in der Datenbank abgelegte Informationen, z.B. zu gefährlichen Ergebnissen oder zu Funktionsrealisierungen, erweitert werden. Bei umfangreicheren Angaben, die die Möglichkeiten einer tabellarischen Darstellung überschreiten, können „Funktionssteckbriefe“ eine mögliche Darstellungsform sein (s.a. Anhang 8).

Tabelle 28: Ergebnis-/Ausgabebeispiel „Funktionsliste“

Nummer und Funktionsname				Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
				Ausführung, um …	Abkürzungen s. Fußnote[41]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	Fahrwegsicherung			… einen freien Fahrweg einzustellen und gegenüber anderen Fahrzeugen / Fahrzeugverbänden sowie querenden Dritten zu sichern.	Die zwischen einem Start- und einem Zielpunkt liegenden Fahrwegelemente müssen frei von anderen Beanspruchungen sein, d.h. andere Beanspruchungen ausgeschlossen sein (FWS-1). Die beweglichen Fahrwegelemente müssen sich in der erforderlichen Lage befinden (FWS-2) und der Fahrweg gegen kreuzende Dritte gesichert sein (FWS-3).	Fgr	Gesicherter Fahrweg	„Fahrweg ist gesichert“	s. zugehörige Funktion
FWS	1	Ausschluss konkurrierender Fahrwegelementbeanspruchung		… untereinander unverträgliche Beanspruchungen von Fahrwegelementen durch Fahrzeuge oder Fahrzeugverbände auszuschließen.	Der Ausschluss konkurrierender Beanspruchungen beruht auf einer Entscheidung über die Zulässigkeit beabsichtigter Beanspruchungen und dem Befolgen der Entscheidung. Ein Fahrwegelement darf nur zur Beanspruchung freigegeben werden, wenn es frei von anderen Beanspruchungen ist. Dazu müssen alle Formen der Fahrwegelementbeanspruchung ermittelt (FWS-1.1) und über die Zulassung einer neuen Beanspruchung entschieden werden (FWS-1.2).	BGrF	Ausschluss konkurrierender Fahrwegelementbeanspruchung	„konkurrierende Beanspruchung ist ausgeschlossen“	Summe des Inputs der zugeordneten Teilfunktionen
FWS	1	1	Beanspruchungsermittlung	… alle Formen der Beanspruchung von Fahrwegelementen durch andere Fahrzeuge / andere Fahrzeugverbände zu erfassen.	Zum Ausschluss konkurrierender Fahrwege müssen alle Formen der Fahrwegbeanspruchung ermittelt werden. In Abhängigkeit davon, wo sich das nutzende Fahrzeug befindet, ergeben sich unterschiedliche Beanspruchungsformen: Fahrzeug auf dem Fahrwegelement (FWS-1.1.1), Fahrzeug in Annäherung an das Fahrwegelement (FWS-1.1.2), Inanspruchnahme benachbarter lichter Räume (FWS-1.1.3).	BTf	Wert des Beanspruchungszustands	„Fahrwegelement nicht beansprucht“ „Fahrwegelement beansprucht“	Summe des Inputs der zugeordneten Teilfunktionen

[41] BGrF = Betriebliche Grundfunktion, BTf = Betriebliche Teilfunktion , Fgr = Funktionsgruppe

5.2 Beispiele für die Analyse definierter Funktionen

Die im Abschnitt 5.1 beispielhaft aufgeführten Funktionen sind im Hinblick auf eine generische Referenz für Betriebsverfahren mit dem im Kapitel 4 entwickelten Vorgehen zielgerichtet als betriebliche Funktionen definiert worden. Folgerichtig ist dabei nur zwischen Funktionsgruppen, betrieblichen Grundfunktionen und betrieblichen Teilfunktionen unterschieden worden.

Am Beispiel dreier in [BEP08] als Ergänzung zur prEN 15380-4 definierten Funktionen wird nachfolgend gezeigt, wie das entwickelte Vorgehen auch zur Analyse und Klassifizierung bereits definierter Funktionen herangezogen werden kann.[42] Da diese Funktionen, wie die Analyse im Abschnitt 3.2.3 ergeben hat, überwiegend schlagwortartig formuliert worden sind, werden die Zwecke mit Hilfe eines realisierungsunabhängigen Finalsatzes nachträglich definiert, um im Sinne der IEC 61226 eine eindeutige betriebliche Zweckbestimmung sicherzustellen. Anhand der Zweckbestimmung erfolgt eine Einstufung in das bereits im Abschnitt 5.1 verwendete Klassifizierungsschema betrieblicher Funktionen. Dies erlaubt einen Abgleich mit den dort (in 5.1) definierten Funktionen.

Beispiel „LBB Provide track vacany detection“

Für diese Funktion werden in [BEP08] als Realisierungsbeispiele Gleisstromkreise und Achszähleinrichtungen angegeben. Daraus ist zu schließen, dass die Funktion ausgeführt wird, um die physikalische Besetzung eines Gleis(abschnitt)es zu ermitteln. Sie entspricht damit exakt der im Abschnitt 5.1.3, Bild 40 als Beispiel angeführten Funktion FWS-1.1.1, die im Rahmen des Ausschlusses konkurrierender Fahrwegelementbeanspruchungen (FWS-1) neben weiteren Funktionen einen Beitrag zur Ermittlung der Fahrwegelementbeanspruchung (FWS-1.1) liefert. Dementsprechend ist „Provide track vacany detection“ als betriebliche Teilfunktion einzustufen. Ihr Versagen ist eine Ursache für das Versagen des Ausschlusses konkurrierender Fahrwegelementbeanspruchungen.

→ Zweck: Ausführung, um Fahrzeuge / Fahrzeugverbände zu erfassen, die sich physikalisch auf den Fahrwegelementen befinden.

→ Klassifizierung: Betriebliche Teilfunktion (BTf)

→ Abgleich mit Funktionen gemäß 5.1: entspricht FWS-1.1.1 „Besetzungsermittlung“; die auf der gleichen Ebene liegenden Funktionen FWS-1.1.2 „Belegungsermittlung“ und FWS-1.1.3 „Profilkonflikterkennung“ werden nicht abgedeckt.

[42] Weitere Beispiele befinden sich in Anhang 7.

Beispiel „LBC Provide positioning information“

Der Zweck der Funktion „Provide positioning information“ lässt sich unmittelbar angeben: Sie wird ausgeführt, um dem Fahrzeug den Ist-Ort zu übermitteln. Die Kenntnis des Ortes kann als eine allgemeingültige Voraussetzung zum Bewegen von Fahrzeugen auf einer Infrastruktur angesehen werden. Die Funktion darf deshalb als generisch für alle Verkehrssysteme angesehen werden. Der Bezug zum Betriebsprozess bleibt offen und kann erst durch die betriebliche Funktion hergestellt werden, die die Ortsinformation nutzt. Die Funktion „Provide positioning information“ ist deshalb als betriebliche Teilfunktion einzustufen. Dies zeigt sich auch in der FMEA, da die Versagen der Funktion zwar in Form von Differenzen zum Ist-Ort angegeben werden können, die Versagensfolgen aber nur im Zusammenhang mit der die Ortsinformation nutzenden Funktion angegeben und beurteilt werden kann. Eine falsche Ortsinformation kann z.B. in einem Fall eine Ursache für das Versagen einer Funktion sein, die der Geschwindigkeitsregelung dient, und in einem anderen Fall eine Ursache für das Versagen eines Beanspruchungsausschlusses für ein Fahrwegelement.

→ Zweck: Ausführung, um einem Fahrzeug den Ist-Ort zu übermitteln

→ Klassifizierung: Betriebliche Teilfunktion (BTf)

→ Abgleich mit Funktionen gemäß 5.1: Teil mehrerer betrieblicher Grundfunktionen, kann u.a. für FWS-1.1 „Beanspruchungsermittlung“ und z.B. auch innerhalb der Funktionsgruppe FZS „Fahrzeugsteuerung“ genutzt werden

Beispiel „LBD Provide wayside train protection“

Der Zweck einer streckenseitigen Zugsicherung wird in [BEP08] nicht explizit angegeben. Anhand der als Beispiele angeführten Einrichtungen können jedoch für die definierte Funktion „Provide wayside train protection“ zwei grundsätzliche Ziele abgeleitet werden. Die Ausführung erfolgt, um

a) das gefährliche Überschreiten vorgegebener Fahrrestriktionen zu verhindern und/oder

b) nach dem Überschreiten vorgegebener Fahrrestriktionen das Eintreten eines Unfalls zu vermeiden.

Aus beiden Formulierungen wird deutlich, dass der verfolgte Zweck in einem Zusammenhang mit dem Ausführen anderer Funktionen zu sehen ist, deren Versagen zu der Verletzung der vorgegebenen Fahrrestriktionen führen kann. Der Zweck ist nicht unmittelbar betrieblich, d.h. im Sinne einer Ortsveränderung, motiviert. Eine Klassifizierung als betriebliche Grundfunktion oder als betriebliche Teilfunktion scheidet deshalb aus.

Die durch die Formulierungen ausgedrückten Funktionen dienen ausschließlich der Verbesserung der Sicherheit betrieblicher Funktionen, greifen dazu jedoch an zwei verschiedenen Stellen in die Wirkungskette ein. Nach 4.4.4 ist a) folglich als Prüf- und Kontrollfunktion und b) als Abfangfunktion zu klassifizieren. Unter generischen Gesichtspunkten sollten deshalb beide bezweckten Ziele als getrennte Funktionen einer Funktionsgruppe mit dem Namen

„Train protection / Zugbeeinflussung“ definiert werden. Ob sie in einem realen System überhaupt und wenn, einzeln oder gemeinsam durch einen oder mehrere Funktionsträger realisiert werden, ist eine Entscheidung, die entsprechend der systemspezifischen Einsatz- und Randbedingungen zu treffen ist.

→ Zweck a): Ausführung, um das gefährliche Überschreiten vorgegebener Fahrrestriktionen zu verhindern und/oder

→ Zweck b): Ausführung, um nach dem Überschreiten vorgegebener Fahrrestriktionen das Eintreten eines Unfalls zu vermeiden

→ Klassifizierung: a) Prüf- und Kontrollfunktion (PrKoF) und b) Abfangfunktion (AbF)

→ Abgleich mit Funktionen gemäß 5.1: keine Entsprechung

5.3 Erkenntnisse

Betriebsverfahren sind komplexe funktionale Systeme, die sehr unterschiedlich realisiert werden können. Für eine generische Beschreibung ist nicht nur das Lösen von realisierungsspezifischen Fachtermini, sondern auch von den Systemarchitekturen erforderlich, da sie i.d.R. Funktionsrealisierungen implizieren. Aus der Anwendung der im Kapitel 4 entwickelten Grundlagen zur Definition einer generischen Referenz lassen sich die nachfolgend aufgeführten Erkenntnisse ableiten.

Allgemein

- Mit dem entwickelten Vorgehen sind Grundlagen zur Definition einer generischen Referenz für die Betriebsverfahren spurgeführter Verkehrssysteme geschaffen worden. Sie zeigen einen Weg auf, um einerseits in einem für generische Betrachtungen erforderlichen Maße von bestehenden Systemlösungen zu abstrahieren, andererseits aber auch in umgekehrter Richtung wieder auf sie als Realisierungsoptionen verweisen zu können.
- Die prinzipielle Anwendbarkeit der geschaffenen Grundlagen konnte nicht nur unter Laborbedingungen, sondern auch in einem praxisnahen Projekt unter Einbeziehung einer 10-köpfigen Expertengruppe aus den Bereichen der Leit- und Sicherungstechnik und der betrieblichen Regelwerke gezeigt werden.
- Im Rahmen der Praxisanwendung wurden innerhalb des infrastrukturseitigen Teils der Betriebsverfahren für fünf Funktionsgruppen betriebliche Grundfunktionen und betriebliche Teilfunktionen generisch definiert. Die der Funktionsgruppe Fahrwegsicherung (FWS) werden im Rahmen dieser Arbeit als Beispiele mit dem Status „Entwurf“ vorgelegt (Anhänge 5, 6).
- Eine generische Referenz für Betriebsverfahren kann und darf sich weder auf bekannte Systemarchitekturen und Systemrealisierungen noch auf die i.d.R. mit lösungsspezifi-

schen Bedeutungen belegten Fachtermini oder andere Schlagworte stützen. Die geschaffenen Grundlagen bieten mit ihrer zweck- und wirkungskettenorientierten Betrachtungs- und Beschreibungsweise einen Weg, das betrachtete System auf funktionaler Basis zu strukturieren.

- Der notwendige Verzicht auf Schlagworte und Realisierungsbeispiele führt zu einem etwas erhöhten Beschreibungsumfang je Funktion. Es empfiehlt sich daher, die generische Referenz in Form einer Datenbank anzulegen, um den Erfordernissen der jeweiligen Anwendergruppe nur die für sie erforderlichen Informationen zur Verfügung stellen zu können.

Zur Formulierung generischer Funktionsdefinitionen

- Die Formulierung von Funktionen als adverbiale Bestimmung des Zwecks in Form eines Finalsatzes führt im Vergleich zur Verwendung von Schlagworten zu eindeutig zweckbestimmten Funktionsformulierungen. Die Anforderungen der IEC 61226 an eine Funktionsdefinition werden konsequent und in einheitlich aufgebauter Form erfüllt.
- Im Vergleich zu Schlagworten fallen die Funktionsdefinitionen etwas umfangreicher aus, doch beginnend mit den einführenden Worten „Ausführung, um …“ kann ihr Umfang auf ein auch in Tabellen verträgliches Maß reduziert werden.
- Die Formulierung von Funktionen als Finalsatz erlaubt nicht nur den Verzicht auf die Nennung des Funktionsträgers, sondern auch auf die Angabe einer Tätigkeit. Lediglich das realisierungsunabhängige Wort „Ausführung“ weist darauf hin, dass (irgend)etwas getan werden muss, um den definierten Zweck zu erreichen.
- Funktionsnamen erlauben zwar eine griffige Benennung der definierten Funktionen, sie sind i.d.R. aber nicht mehr eindeutig als Zweckformulierung zu erkennen. Sie sollten deshalb nie allein, sondern nur im Zusammenhang mit der Zweckbestimmung aufgeführt werden.
- Mit den geschaffenen Grundlagen kann in generischen Funktionslisten auf die Angabe von Realisierungsbeispielen verzichtet werden, ohne dass ihre Aussagekraft z.B. gegenüber der der Vornorm prEN 15380-4 zurücksteht. Realisierungsbeispiele werden nicht zur Definition der Funktion oder zu deren Erläuterung benötigt, sondern können optional als Referenzen angegeben werden, um z.B. unterschiedliche Formen der Realisierung der definierten Funktionen zu vergleichen.

Zur Definition des erforderlichen funktionalen Systems

- Das Definieren einer generischen Referenz für Betriebsverfahren setzt eine umfassende Systemdefinition voraus, um die Beziehungen der Funktionen untereinander und zur funktionalen Umgebung des betrachteten Systems beschreiben zu können.

- Die Funktionsliste der prEN 15380-4 bietet bezogen auf Betriebsverfahren keine ausreichende Grundlage, um eine entsprechende funktionale Systemdefinition zu schaffen, da sie nur die aus fahrzeugseitiger Sicht an den Schnittstellen zum Betriebsverfahren notwendigen Funktionen enthält, die für das Zusammenwirken eines einzelnen Fahrzeugs mit dem Betriebsverfahren notwendig sind. Aus infrastrukturseitiger Sicht besteht die originäre Aufgabe eines Betriebsverfahrens jedoch vorrangig darin, die Fahrten mehrerer Fahrzeuge so zu koordinieren, dass sie sicher durchgeführt werden können. Der dazu notwendige Ausschluss konkurrierender Fahrwegelementbeanspruchungen bildet den infrastrukturseitigen Kern der Betriebsverfahren, enthält aber der anderen Sicht wegen – konsequenter Weise – keine Entsprechung in der Fahrzeugnorm prEN 15380-4.
- Die für das Definieren einer generischen Referenz benötigte funktionale Systemdefinition darf, um keine Systemlösungen zu implizieren, nicht auf einer aus Subsystemen bestehenden Systemarchitektur abgestützt werden. Mit den geschaffenen Grundlagen können auf Basis funktionaler Betrachtungen zu den benachbarten funktionalen Systemen generische Ersatzstrukturen geschaffen werden, innerhalb derer das funktionale System top-down verfeinert werden kann.

Wahrnehmung des funktionalen Systems

- Die in den geschaffenen Grundlagen enthaltene stringente Zweckorientierung verschiebt den Fokus der Systembetrachtung von den mehr realisierungsnahen Fragen, wer etwas macht oder wie etwas gemacht wird hin zu der generischen Frage, warum etwas gemacht wird. Dadurch wird das Augenmerk auf weitere Differenzierungsmöglichkeiten zur Strukturierung des betrachteten funktionalen Systems gelenkt. Dies gilt insbesondere für die Unterscheidung zwischen Funktionen, die für die Abwicklung der Ortsveränderung von Personen und Gütern erforderlich sind und Funktionen, die „nur“ benötigt werden, um das mit dem Herbeiführen der Ortsveränderung einhergehende Risiko zu senken. Gerade bei letzteren ist zu vermuten, dass sie hinsichtlich ihrer Realisierungsformen verhältnismäßig stark variieren, weil sie häufig auf Grund (un-)fallspezifischer Erfahrungen „nachgerüstet“ worden sind. Ihr Zweck hingegen wird weitgehend übereinstimmend in dem Eingriff in die von einem Fehler oder Ausfall zu einem Unfall verlaufende Wirkungskette bestehen.
- Die Identifizierung gefährlicher Ergebnisse wird für die Definition der generischen Referenz nicht unmittelbar benötigt. So haben ihre Ergebnisse z.B. keinen Eingang in die Funktionsliste (Anhang 5) gefunden. Mittelbar hat sie den Definitionsprozess jedoch unterstützt, weil im Rahmen der Folgenanalyse die für das betrachtete System definierten funktionalen Wirkungszusammenhänge nachvollzogen werden konnten. Dadurch ergaben sich Möglichkeiten zu Plausibilitätskontrollen hinsichtlich der Definition und der Klassifizierung der betroffenen Funktionen.

Zur Arbeitsweise

Die mit dieser Arbeit geschaffenen Grundlagen können für sich allein weder ein vollständiges noch ein inhaltlich korrektes Ergebnis von Funktionslisten garantieren. Um diese Ziele möglichst umfassend zu erreichen, ist, wie z.B. bei der Erarbeitung von Normen, die Einbeziehung einer ausreichenden Anzahl von im Fachgebiet ausgewiesenen Experten erforderlich. Es war dem Autor dieser Arbeit vergönnt, die Ansätze in einem zehnköpfigen Expertenkreis praxisnah anwenden und erste Erfahrungen sammeln zu können. Diese erlaubt die Feststellung, dass die geschaffenen Grundlagen derartige Arbeiten unterstützen, indem sie in dem durch sehr heterogene Systemlösungen geprägten Fachgebiet der Betriebsverfahren unterschiedliche Sichtweisen der Experten kanalisieren und auf einen gemeinsamen, generischen Nenner bringen.

6 Zusammenfassung

Ziel der Arbeit

Für die Fahrzeuge spurgeführter Verkehrssysteme liegt mit der Vornorm prEN 15380-4:2009 eine Liste von Funktionen vor, die mit generischem Anspruch definiert worden sind. Für die Betriebsverfahren spurgeführter Verkehrssysteme gibt es bislang keine vergleichbare Liste. Dies ist auch dem Umstand geschuldet, dass die Betriebsverfahren wegen der vielfältigen Möglichkeiten, Mensch und Technik zu kombinieren, im Vergleich zum Fahrzeugsektor sehr heterogen gestaltbar sind. Gleichwohl besteht das Bedürfnis, z.B. im Rahmen verschiedener Harmonisierungsbestrebungen, die an sich überall gleichen Grundprinzipien des Funktionierens der Eisenbahnen einheitlich zu beschreiben und z.B. für eine mit der prEN 15380-4 vergleichbare Liste generisch zu definieren.

Die besondere Herausforderung einer solchen Aufgabe besteht in dem Überwinden der aufgrund der heterogenen Gestaltung unterschiedlich geprägten Denk- und Betrachtungsweisen. Dementsprechend war es das Ziel der vorliegenden Arbeit, Grundlagen für das Erstellen einer derartigen generischen Referenz zu schaffen, die die an einem solchen Definitionsprozess beteiligten Fachleute beim Abstrahieren von bekannten Systemlösungen unterstützen.

Ergebnisse

Es konnte gezeigt werden, dass es trotz der erforderlichen Abstraktionen von bestehenden Systemlösungen möglich ist, für die Betriebsverfahren spurgeführter Verkehrssysteme ausschließlich auf Basis einer funktionalen Systemdefinition, d.h. ohne eine konkrete Systemarchitektur, eine generische Referenz zu definieren. Dazu sind Grundlagen geschaffen worden, die zum Definieren einer solchen Funktionsliste herangezogen werden können. Sie beruhen auf der konsequenten Anwendung des in der IEC 61226 definierten Funktionsbegriffs, der lediglich am Zweck einer nicht näher zu definierenden Aktion oder Tätigkeit orientiert ist.

Zu den Grundlagen des in dieser Arbeit entwickelten formalisierten Vorgehens gehören natürlichsprachliche Mittel und vorab definierte Funktionsgrundtypen. Beide Elemente unterstützen das Einhalten des für das Definieren generischer betrieblicher Funktionen erforderlichen Abstraktionsgrads bis hin zur Identifizierung ebenfalls generischer Gefährdungen. Der Zweck einer Funktion wird im Sinne der IEC 61226 z.B. durch die Formulierung als adverbiale Bestimmung in Form eines Finalsatzes mit „um … zu …“ hervorgehoben und so eindeutig gegenüber der i.d.R. von der Realisierung abhängigen Funktionsausführung abgegrenzt. Die Funktionsgrundtypen wiederum, ihrerseits ebenfalls über den Zweck definiert, spiegeln die Hauptmotivationen für Aktionen oder Tätigkeiten in spurgeführten Verkehrssystemen wieder:

(1) das Erfüllen des primären Systemzwecks, die Ortsveränderung von Personen und Gütern, und
(2) die Verbesserung der Sicherheit durch das gezielte Eingreifen in die von einem Ausfall oder Fehler bis zu einem Unfall verlaufende Wirkungskette.

Sie dienen nicht nur der Einordnung der zu definierenden betrieblichen Funktionen in das Gesamtsystem, sondern erlauben auch diesbezügliche Plausibilitätsprüfungen bei der Identifizierung gefährlicher Ergebnisse.

Am Beispiel der Definition von Funktionen der Funktionsgruppe „Fahrwegsicherung" wurde das Vorgehen demonstriert. Gleiches gilt für die Analyse bereits definierter Funktionen. Anhand der gezeigten Beispiele wird deutlich, dass es trotz der erforderlichen Abstraktionen von bestehenden Systemlösungen möglich ist, ausschließlich auf Basis einer funktionalen Systemdefinition, d.h. auch bei Verzicht auf eine konkrete Systemarchitektur, einen festen Orientierungsrahmen zu definieren, der im Sinne einer generischen Referenz genutzt werden kann.

Nutzen

Ein erster praktischer Nutzen generisch definierter betrieblicher Funktionen konnte bereits bei der Wiederzulassung des Betriebs auf der Transrapid-Versuchstrecke im Emsland (TVE) gezeigt werden. Die Analyse des dortigen betrieblichen Regelwerks ist, einer Idee des Autors dieser Arbeit folgend, auf einer solchen generischen Basis durchgeführt worden. Die generisch definierten Funktionen erlaubten nicht nur eine gezielte Abfrage und Analyse der auf der TVE gewählten Lösungsansätze, sondern auch jener bei den herangezogenen Referenzsystemen (vgl. a. [BG08]).

Dieses Beispiel unterstreicht einen möglichen Nutzen einer Liste generisch definierter Funktionen z.B. für Aufsichtsbehörden. Die verbesserte Vergleichbarkeit kann vergleichende Sicherheitsnachweise beschleunigen, weil auf der Basis einheitlich definierter Funktionen verschieden realisierte Systemlösungen verglichen werden können. So wird ihrer Entwicklung seitens der deutschen Aufsichtsbehörde, dem Eisenbahn-Bundesamt, mit Interessen entgegengesehen[43].

Ausblick

Die im Rahmen eines Projekts[44] definierte und in dieser Arbeit in Teilen veröffentlichte Liste betrieblicher Funktionen, ihr Aufbau als auch die in ihr enthaltenen Formulierungen dürfen jedoch noch nicht als endgültig aufgefasst werden, sondern sind als Entwurf anzusehen. Als unmittelbar folgende Arbeits- und Forschungspunkte sind die Validierung im internationalen

[43] Gespräch des Autors der vorgelegten Arbeit und Vertretern der Deutsche Bahn AG beim Eisenbahn-Bundesamt in München am 12.12.2008.

[44] Siehe Kapitel 5 „Anwendung"

Kontext, der Aufbau einer datenbankgestützten Sammlung von Realisierungsbeispielen sowie der Nachweis der Vollständigkeit zu nennen. Ferner ist die Frage zu klären, bis zu welcher Grenze die Funktionsstruktur verfeinert werden kann, ohne den generischen Anspruch zu verlieren.

Als ein wichtiger und grundlegender Schritt für diese Arbeiten ist der Auf- und Ausbau einer Datenbank generisch definierter betrieblicher Funktionen anzusehen, die auch die Referenzen zu unterschiedlichen Realisierungen enthält. Bereits sie kann die Vereinheitlichung von Denkstrukturen und Begrifflichkeiten fördern und somit z.B. zur Harmonisierung der Eisenbahnlehre wie auch zur Entwicklung einheitlicher Regelwerksstrukturen beitragen. Auch ist zu erwarten, dass sie, als Ausgangsbasis für generische Ereignisbäume herangezogen, zur Vereinheitlichung von Risikoanalysen und deren effizienterer Durchführung beitragen kann.

Basierend auf einer solchen Datenbank ist in einem weiteren Schritt das Zusammenfügen der definierten Funktionen zu einer Art Basisbetriebsverfahren vorstellbar, das als Referenz für die Entwicklung neuer und Weiterentwicklung bestehender Betriebsverfahren dienen könnte. Eine Herausforderung dürfte dabei auch in der Frage liegen, inwieweit in einem Modell die bei der Realisierung durchaus unterschiedlichen Möglichkeiten zur Kombination der Funktionen abgebildet werden können. Gemessen an dem beinahe über zwei Jahrhunderte eher evolutionären Zustandekommen der heutigen, z.T. sehr unterschiedlichen Betriebsverfahren, würde mit der systematischen Ableitung eines generischen Kerns für Betriebsverfahren Neuland betreten, das durchaus als problemorientierte Grundlagenforschung angesehen werden darf.

Literaturverzeichnis

[2001/16/EG] Richtlinie 2001/16/EG des europäischen Parlaments und des Rates vom 19. März 2001 über die Interoperabilität des konventionellen transeuropäischen Eisenbahnsystems. Amtsblatt der Europäischen Gemeinschaften 2001

[2006/62/EG] Verordnung (EG) Nr. 62/2006 der Kommission vom 23. Dezember 2005 über die technische Spezifikation für die Interoperabilität (TSI) zum Teilsystem „Telematikanwendungen für den Güterverkehr“ des konventionellen transeuropäischen Eisenbahnsystems. Amtsblatt der Europäischen Union 2006

[2006/679/EG] Entscheidung der Kommission vom 28. März 2006 über die Technische Spezifikation für die Interoperabilität (TSI) zum Teilsystem „Zugsteuerung/Zugsicherung und Signalgebung“ des konventionellen transeuropäischen Eisenbahnsystems. Amtsblatt der Europäischen Union 2006

[2006/860/EG] Entscheidung der Kommission vom 7. November 2006 über die technische Spezifikation für die Interoperabilität des Teilsystems „Zugsteuerung, Zugsicherung und Signalgebung“ des transeuropäischen Hochgeschwindigkeitsbahnsystems. Amtsblatt der Europäischen Union 2006

[2006/920/EG] Entscheidung der Kommission vom 11. August 2006 über die technische Spezifikation für die Interoperabilität des Teilsystems „Verkehrsbetrieb und Verkehrssteuerung“ des konventionellen transeuropäischen Eisenbahnsystems. Amtsblatt der Europäischen Union 2006

[2008/57/EG] Richtlinie 2008/57/EG des europäischen Parlaments und des Rates vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft (Neufassung). Amtsblatt der Europäischen Union 2008

[2008/232/EG] Entscheidung der Kommission vom 21. Februar 2008 über die technische Spezifikation für die Interoperabilität des Teilsystems „Fahrzeuge“ des transeuropäischen Hochgeschwindigkeitsbahnsystems. Amtsblatt der Europäischen Union 2008

[BEP08] Bepperling, Sonja-Lara: Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik. Dissertation, Technische Universität Braunschweig 2008, http://www.digibib.tu-bs.de/?docid=00024255

[BG08] Bosse, Gunnar; Gayen, Jan-Tecker: Realisierungsunabhängige Identifizierung von Gefährdungen auf Basis betrieblicher Funktionen spurgeführter Verkehrssysteme. ZEVrail Glasers Annalen 132 (2008) 4, S. 116-127

[BP01] Bosse, Gunnar; Pierick, Klaus: Unfall ICE 884. Gutachten zum Fahrtverlauf und zum Unfallhergang im Auftrag der Staatsanwaltschaft Lüneburg (161 Js 12212/98), Braunschweig 2001

[BRA05] Braband, Jens: Risikoanalysen in der Eisenbahnautomatisierung. Eurailpress Tetzlaff-Hestra GmbH & Co. KG, Hamburg, 2005

[BRA08] Braband, Jens: Einheitliches Risikoakzeptanzkriterium für technische Systeme bei europäischen Bahnen. Signal + Draht (100) 7+8/2008, S. 25-29

[BRA10] Brandau, Jochen: Schnittstelle zwischen Mensch und Technik. Deine Bahn 1/2010, S. 11-14

[CLC/TR 50126-2] CENELEC: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) -Part 2: Guide to the application of EN 50126-1 for safety. 2/2007

[DB01] Deutsche Bahn AG: RA FunkFahrBetrieb, Gefährdungskatalog V3.4 vom 26.01.2001

[DB02] Deutsche Bahn AG: Risikoanalyse Elektronisches Stellwerk, Gefährdungsidentifikation V2b vom 07.11.2002

[DEM79] DeMarco, Tom: Structured Analysis and System Specification. Prentice Hall, 1979

[DIN 40041] DIN 40041: Zuverlässigkeit; Begriffe. 12.1990

[EN 50126] Bahnanwendungen: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS). Beuth Verlag GmbH, Berlin März 2000

[EN 50129] Bahnanwendungen: Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik. Beuth Verlag GmbH, Berlin Oktober 2003

[EN 60812] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und –auswirkungsanalyse (FMEA) (IEC 60812:2006), 2006

[ERA07] Europen Railway Agency: Recommendation on the 1st set of Common Safety Methods. 12/2007.

[FP90] Fricke, Hans; Pierick, Klaus: Verkehrssicherung. Teubner, Stuttgart 1990

[HL09] Hecht, Markus; Luther, Doris: Aktive und passive Sicherheit der Eisenbahn heute und morgen. Der Eisenbahningenieur 11/2009

[IEC 60812] Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). Beuth Verlag GmbH, Berlin, 2001

[IEC 61226] Nuclear power plants – Instrumentation and control systems important to safety –Classification of instrumentation and control functions, International Electrotechnical Commission, 2005

[IEC 61508-4] IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations. International Electrotechnical Commission, Draft 2008

[IEC 62267-2] IEC 62267-2 TR Ed. 1: Railway applications – Automated guided urban transport (AUGT) – Safety requirements – Part 2: Hazard analysis at top system level. International Electrotechnical Commission, Draft 2010

[IfEV01] Institut für Eisenbahnwesen und Verkehrssicherung: Unsere Lehre im Eisenbahnwesen – eine Dreiecksgeschichte. http://www.tu-braunschweig.de/ifev/lehre, Stand 2008-01-17

[KPG08] Klinge, Karl-Albrecht; Püttner, Rüdiger; Geisler, Marc; Schütte, Jörg: ROSA - Optimierende Sicherheitsanalyse System Bahn. Erschienen in: Schienenverkehr - sicher, leise, effizient; herausgegeben vom Bundesministerium für Wirtschaft und Technologie, 10115 Berlin, 2008

[LHB03] Leißner, Frank; Hansen, Lars Hauke; Beck, Rainer; Kammel, Karl: Erkenntnisse aus der Risikoanalyse für die ETCS-Pilotanwendung. Signal und Draht 6/2003; S. 6 - 10

[MAS09] Maschek, Ulrich: Eine generische Sicht auf die Betriebssicherheit im spurgeführten Verkehr. Eisenbahningenieur 2/2009, S. 36-40

[MIL09] Milius, Birgit: Die Konstruktion eines semi-qualitativen Risikographen. Dissertation, Technische Universität Braunschweig 2009, http://www.digibib.tu-bs.de/?docid=00031882

[NP02] Naumann, Peter; Pachl, Jörn: Leit- und Sicherungstechnik im Bahnbetrieb. Tetzlaff Verlag, 2002

[PAC05] Pachl, Joern: Railway Operation and Control. VTD Rail Publishing, Mountlake Terrace (USA), 2nd printing 2005

[PAC08] Pachl, Jörn: Betriebsführung. In: Handbuch Das System Bahn, Eurail Press, 1. Auflage 2008, S. 505-550

[PAC08-1] Pachl, Jörn: Sicherheitsbetrachtungen im Bahnbetrieb. Vorlesung Bahnsicherungstechnik. http://rzv113.rz.tu-bs.de/dllep/pachl/BST_2.pdf, Stand 2008-11-16

[PAC08-2] Pachl, Jörn: Glossar der Systemtechnik des Schienenverkehrs. http://joernpachl.gmxhome.de/glossar.htm, Stand 2008-12-06

[PAC08-3] Pachl. Jörn: Betriebsverfahren im internationalen Vergleich. Gastvorlesung an der TU Dresden, 2008

[PAC08-4] Pachl, Jörn: Die Bedeutung betrieblicher Regelwerke für die Leit- und Sicherungstechnik. Signal + Draht (100) 12/2008, S. 32-38

[POT88] Pottgießer, Hans: Sicher auf den Schienen. Birkhäuser Verlag, Basel 1988

[prEN 15380-4] CENELEC – prEN 0015380-4, Railway applications – Classification system for rail vehicles – Part 4: EN 0015380

Part 4: Function groups, Draft, June 2007.

[SCH02] Schivelbusch, Wolfgang: Geschichte der Eisenbahnreise, Zur Industrialisierung von Raum und Zeit im 19. Jahrhundert. Fischer Taschenbuch Verlag, Frankfurt am Main, 2. Auflage 2002

[UIC07] UIC: Generic Hazard List Methodology for Railway Signalling. Union Internationale des Chemins de Fer, Paris 2007

[VDV 331] Sicherheitsbetrachtungen und Anforderungsklassen für Signal- und Zugsicherungsanlagen gemäß BOStrab, VDV-Richtlinie 331, 1994

[WK07] Weber, Ulrich; Kurz, Sonja-Lara: Funktionale Systemdefinition anhand der EN 0015380-4. Vortrag, Bieleschweig-Workshop, Braunschweig 10/2007 http://rzv113.rz.tu-bs.de/Bieleschweig/B10/1_Weber.pdf

Anhang 1: Analyse der „Starting Point Hazards“ (ROSA)

In der folgenden Tabelle werden beispielhafte Starting Point Hazards aus dem Projekt „ROSA“ [KPG08] entsprechend der Art ihrer Formulierung gruppiert. Die Art ihrer Formulierung wird erläutert und beurteilt, ob es sich um eine funktional abgeleitete Gefährdungsformulierung handelt, d.h. ob ihnen Funktionsdefinitionen zugrunde liegen.

Starting Point Hazards (SPH)	**Beurteilung**
Broken wheel, *broken axle,* *broken switch component,* *Failure of vehicle frame/car body*	Als Gefährdungen sind eingetretene Bauteilversagen formuliert worden, denen bereits gefährliche Funktionsversagen, hier im Sinne des Versagens von Tragen und Führen, vorausgegangen sind. Im Falle gebrochener Räder oder Achsen liegt bereits ein Unfall vor. Betrieblich gesehen handelt es sich um nicht gewollte Zustände von fahrzeug- bzw. fahrwegseitigen „Hardwarekomponenten“ des Systems Eisenbahn. Sie sind aus betrieblicher Sicht „gefährlich“, weil sie während des Betriebs auftreten und zu Unfällen führen können bzw. bereits geführt haben. Die Ursachen und Entwicklungen, die zu diesen Zuständen führen, müssen fahrzeug- und fahrwegseitig durch die entsprechenden Systemrealisierungen beherrscht werden, denn aus betrieblicher Sicht kann lediglich versucht werden, die eingetretenen betrieblich gefährlichen Zustände zu detektieren und den Betrieb wieder in einen sicheren Zustand zu überführen. Den SPH liegen keine Funktionen zugrunde, die den Betriebsverfahren zuzurechen sind.
Authorised person crosses track, *Staff working on track,* *Staff working near track e.g. neighboured track,* *Road traffic user on LC,* *Possibility of passenger leaning out of window*	Diese SPH-Formulierungen sind situativ aufgebaut. Es handelt sich um Formulierungen von Situationen, die für das System Eisenbahn und seinen Betrieb typisch sind. Sie sind im System erforderlich und, wie z.B. mit dem Wort „authorised“ unterstrichen wird, zulässig. Aus diesem Grunde dürfen sie von sich aus auch nicht gefährlich sein. Sie stehen allerdings potenziell im Konflikt mit dem Betrieb von Fahrzeugen und müssen deshalb innerhalb der Betriebsverfahren mit Hilfe geeigneter betrieblicher Funktionen beherrscht werden. Erst im Zusammenhang mit dem gefährlichen Versagen dieser in ROSA nicht formulierten betrieblichen Funktionen können sich aus ihnen Unfälle entwickeln. Beispiel: *Road traffic user on LC* beschreibt eine situativ zulässige Situation, denn sie entspricht dem Zweck eines Bahnübergangs. Zur Beherrschung der Situation wird allerdings eine betriebliche Grundfunktion „Bahnübergang sichern“ benötigt. Deren gefährliches Versagen lautet: „Bahnübergang nicht gesichert“. In der Folge könnte sich dann ungewollt die formulierte Situation einstellen. Die SPH sind nicht funktional abgeleitet worden.

Starting Point Hazards (SPH)	**Beurteilung**
Possibility of train rolls away, *possibility of train moving during passenger exchange* *Possible wrong route for train,* *possibility of person falling out of door onto wall*	Dies sind mögliche Folgen von Gefährdungen. Sie können sich nur ergeben, wenn bereits entsprechende Funktionen versagt haben. Es handelt sich damit um die Folgenformulierungen, die entweder bereits Unfälle sind oder die in ihrer weiteren Entwicklung zu einem Unfall führen können. Die Formulierung als Möglichkeit ist nicht notwendig, denn das Eintreten einer Gefährdung ist stets mit einer Wahrscheinlichkeit verbunden, wodurch die Möglichkeit des Eintretens bereits automatisch ausgedrückt wird. Zudem ist eine Gefährdung dadurch gekennzeichnet, dass eine bestimmte Situation bereits eingetreten ist, d.h. eine Systemabweichung vorliegt. Die reine Möglichkeit hierzu ist nicht maßgebend. Die SPH sind nicht unmittelbar aus einer Funktionsdefinition abgeleitet worden.
wrong switch command, *wrong braking distance determined,* *wrong speed profile,* *wrong braking curves*	Diese Gefährdungen sind als Ergebnisse fehlerhaft ausgeführter, aber nicht genannter Funktionen formuliert worden. Sie sind zugleich Ursachen für übergeordnete Funktionen, wie z.B. „Stellen beweglicher Fahrwegelemente“. Die SPH sind können unmittelbar aus einer Funktionsdefinition abgeleitet worden sein.
Slipstream effects on ballast, *Aerodynamic forces impact on train*	Es handelt sich um Beschreibungen von zu beherrschenden Situationen oder Randbedingungen. Sie werden beim Versagen der zu ihrer Beherrschung erforderlichen Funktionen wirksam. Sollen beispielsweise die aerodynamischen Kraftspitzen durch eine Geschwindigkeitsbegrenzung beherrscht werden, bedarf es einer entsprechenden betrieblichen Funktion. Deren gefährliches Versagen kann infolge der dann auftretenden Kraftspitzen zu einem Unfall führen. Die SPH sind nicht funktional abgeleitet worden.

Anhang 2: Analyse der prEN 15380-4 (Code „G“)

Es wird anhand von Auszügen analysiert, inwieweit die in der prEN 15380-4 unter „Code G“ aufgeführten Funktionen für Betriebsverfahren relevant sind oder auf sie übertragen werden können.

prEN 15380-4						**Beurteilung der funktionalen Relevanz für Betriebsverfahren (Bv)**	
CODE			**f**	**Function**		**Erläuterung**	**Zuordnung**
			e	**Example/Explanation**			
G	*B*		*f*	*Provide acceleration and dynamic brake force*		Das Erzeugen von Antriebs- und Bremskräften ist den fahrzeugseitigen Funktionen zuzuordnen. Dies wird auch durch die in der prEN 15380-4 aufgeführten Beispiele unterstrichen. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*traction motor, transmission*			
G	*B*	*C*	*f*	*Acquire propulsion demand*		Mit dieser Funktion sollen die vom Fahrer oder technischen Einrichtungen gegebenen Anforderungen an die Bremssteuerung entgegengenommen und weiter verarbeitet werden, um die erforderlichen Kräfte zu erzeugen. Die Anforderung entspricht der Schnittstelle. Die Weiterverarbeitung folgt danach, ist somit eine fahrzeugseitige Funktion. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*propulsion demand from driver, ATO, internal speed control, brake demand for dynamic brake force from brake control*			
G	*C*		*f*	*Provide deceleration and keep the train at standstill*		Das Erzeugen der Kräfte zum Abbremsen und zur Stillstandsicherung geschieht erst nach der Anforderung. Es ist somit ein zuginterner Prozess, der durch fahrzeugseitige Funktionen zu erfüllen ist. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*braking*			
G	*C*	*B*	*f*	*Get status of braking systems*		Die Ermittlung des Zustandes des Bremssystems ist ein zuginterner Prozess, der benötigt wird, um die Anforderung von Bremsleistungen erfüllen zu können. Er ist durch fahrzeug-seitige Funktionen zu erfüllen. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*also: isolate braking devices*			

G	*C*	*C*	*f*	*Acquire brake demand*	Hierunter wird die Entgegennahme und Umsetzung der vom Fahrer, von Zugüberwachungssystemen oder Notbremseinrichtungen kommenden Bremsanforderungen durch das Managen der verschiedenen Zugbremsen verstanden. Es geht nicht um das betrieblich motivierte Auslösen einer Bremsanforderung, sondern um die anschließende Verarbeitung der Anforderung durch fahrzeugseitige Funktionen. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*from: driver, brake control, emergency device, train protection functions, ATP, brake signal transition, internal speed control, passengers and crew*		
G	*C*	*D*	*f*	*Prioritise brake demand and select braking mode*	Alle folgenden Teilfunktionen dienen der Sicherstellung, dass betrieblich angeforderte Bremsleistungen durch das Fahrzeug erbracht werden. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*setup (emergency) brake mode*		
G	*C*	*E*	*f*	*Allocate braking effort*	s. vor	FzF
			e	*Calculate needed braking effort*		
G	*C*	*F*	*f*	*Handle braking due to train configuration, brake mode and brake demand*	s. vor	FzF
			e	*i. e. Emergency Brake, Service Brake, Parking Brake*		
G	*C*	*G*	*f*	*Apply and release braking forces*	s. vor	FzF
			e	*detect non-release of braking forces*		
G	*C*	*H*	*f*	*Provide Wheel Slide Protection (WSP)*	s. vor	FzF
			e	*Detect and control sliding*		
G	*D*		*f*	*Improve adhesion*	Maßnahmen zur Verbesserung des Kraftschlussbeiwertes dienen der Erzeugung einer angeforderten Bremskraft. Sie sind ebenso wie die dazu erforderliche Regelung fahrzeugseitig zu erbringen. → funktional dem Fahrzeug zuzuordnen	FzF
			e	*sanding*		

Ergebnis: Die G-Funktionen sind sämtlich funktional dem Fahrzeug zuzuordnen.

Anhang 3: Analyse der prEN 15380-4 (Code „K“)

Es wird anhand von Auszügen analysiert, inwieweit die in der prEN 15380-4 unter „Code K“ aufgeführten Funktionen für Betriebsverfahren relevant sind oder auf sie übertragen werden können.

prEN 15380-4					**Beurteilung der funktionalen Relevanz für Betriebsverfahren (Bv)**	
CODE			**f** **e**	**Function** **Example/Explanation**	**Erläuterung / Anmerkung**	**Zuordnung**
K	*B*		*f* *e*	*Indicate the presence of the vehicle to others*	Diese Funktion wird unmittelbar weder zur Erfüllung der Transportaufgabe noch zur Erzeugung der Fahrzeugbewegung benötigt. Die Anwesenheit eines Fahrzeugs anderen Fahrzeugen/Personen anzuzeigen, dient der betrieblichen Koordination. Dieser betriebliche Zweck wird mit der Formulierung jedoch nicht ausgedrückt. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*B*	*D*	*f* *e*	*Indicate the presence by external lights* *tail-end signal*	Funktional identisch mit übergeordneter Funktion KB, gibt zusätzlich eine Realisierungsrichtung vor. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*C*		*f* *e*	*Provide identification*	Die Formulierung drückt mehr eine betriebliche Anforderung an die Fahrzeugrealisierung als eine betriebliche Funktion aus. Das Identifizieren des Fahrzeugs dient betrieblichen Zwecken, die mit der Formulierung nicht näher spezifiziert werden. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*D*		*f* *e*	*Provide operational communication and train/ground data transmission*	Das Vorhalten von Einrichtungen zur Kommunikation und Datenübermittlung von und zum Fahrzeug ist für sich allein genommen keine betriebliche Funktion. Sie sind Hilfsmittel, um nicht näher spezifizierte betriebliche Funktionen durchführen zu können. → dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*D*	*B*	*f* *e*	*Ensure data interface to trackside signalling system* *train antenna*	s. vor	Bv

K	*D*	*C*	*f* *e*	*Provide train to ground communication* *train radio, GSM-R*	s. vor	Bv
K	*D*	*D*	*f* *e*	*Provide ground to train communication*	s. vor	Bv
K	*E*		*f* *e*	*Provide automatic train protection & control*	Dies ist die Anforderung, fahrzeugseitig bestimmte Systemarchitekturen zu gewährleisten, mit denen nicht näher spezifizierte betriebliche Zwecke oder Ziele erreicht werden sollen. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*E*	*B*	*f* *e*	*Provide interface with ATC*	s. vor	Bv
K	*F*		*f* *e*	*Provide automatic train operation*	Mit der ATO werden betriebliche Funktionen realisiert, die auch in anderer Weise ausgeführt werden können. Insofern wird hier weder eine Funktion beschrieben noch wäre sie aus betrieblich-funktionaler Sicht als generisch einzustufen. Dies ist eine Anforderung, die auf eine bestimmte Realisierungsarchitektur abzielt. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*G*		*f* *e*	*Ensure proper route selection and route signalling* *switch control*	Dies ist eine Funktion, mit der sichergestellt wird, dass eine zulässige Route gewählt und signalisiert wird. Bei Eisenbahnen geschieht dies i.d.R. durch Stellwerke. Die Funktion kann jedoch, wie z.B. bei Straßenbahnen, vom Fahrzeug aus ausgeführt werden. Sie wäre aber auch dann als betriebliche Funktion anzusehen. → dem Bereich der Betriebsverfahren zuzuordnen	Bv
K	*G*	*B*	*f* *e*	*Switch route* *device for working the switches*	Das Einstellen von Fahrwegen ist grundsätzlich eine betriebliche Funktion, die auf sehr unterschiedliche Weisen realisiert werden kann: z.B. Handhebel direkt an den Weichen oder fernbedient aus Stellwerken. Sie kann auch von einem Fahrzeug aus ausgeführt werden. Dazu wäre eine entsprechende Einrichtung auf dem Fahrzeug vorzusehen. Dies würde den betrieblichen Charakter der Funktion jedoch nicht verändern. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv

K	G	C				
			f	*Control signals*	Das Steuern der Signale dient der Übermittlung betrieblicher Informationen an das Fahrzeug. Das (optische) Signal ist eine von mehreren Möglichkeiten, eine betriebliche Funktion im Sinne von „Fahrauftrag erteilen“ zu realisieren. Selbst bei einer Realisierung als Führerstandsignalisierung bliebe der betriebliche Charakter der Funktion davon unberührt. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*activate traffic light signals*		

Ergebnis: Die K-Funktionen sind sämtlich den Betriebsverfahren zuzuordnen.

Anhang 4: Analyse der die prEN 150380-4 ergänzenden Funktionen (Code „L“)

Es wird analysiert, inwieweit die als Ergänzung zur prEN 15380-3 gedachten und in [BEP08] unter „Code K“ aufgeführten Funktionen für Betriebsverfahren relevant sind oder übertragen werden können.

Ergänzungen zur prEN 15380-4 [BEP08]					**Beurteilung der funktionalen Relevanz für Betriebsverfahren (Bv)**	
CODE			**f**	**Function (DE)**	**Erläuterung / Anmerkung**	**Zuordnung**
			e	**Example/Explanation (DE)**		
L	*B*		*f*	*Provide wayside functions* *(Streckenfunktionen steuern und sichern)*	Das Vorhalten oder Bereitstellen einer oder mehrerer Funktionen sind elementare Anforderungen an Systemrealisierungen. Der betriebliche Zweck kommt in der Formulierung nicht zum Ausdruck. Es könnte sich der Formulierung nach auch um eine infrastrukturseitige Funktion im Sinne von „Tragen und Führen“ handeln. Aus dem Gesamtkontext ergibt sich jedoch die funktionale Zuordnung zu den Betriebsverfahren.	Bv
			e	*wayside functions* *(Streckenfunktionen)*		
L	*B*	*B*	*f*	*Provide track vacancy detection* *(Gleisschaltmittel, Gleisfreimeldung)*	Diese Funktion dient dem Vorhalten von Gleisfreimeldeeinrichtungen (vgl. a. deutsche Angaben), wobei neben dem Begriff Gleisfreimeldung explizit Gleisschaltmittel als Funktion aufgeführt werden. Funktional verbirgt sich in diesen Formulierungen die Freiprüfung eines Gleisabschnittes. Diese kann aber auch unabhängig von der Strecke, z.B. durch mündliche Meldeverfahren, Augenschein oder die Auswertung von Ortungsinformationen (s. Teilfunktion LBC) realisiert werden. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*track vacancy detection* *(Gleisstromkreise, Achszähler)*		
L	*B*	*C*	*f*	*Provide positioning information* *(streckenseitige Ortung)*	Aus betrieblicher Sicht bleiben der Zweck bzw. die beabsichtigten Ziele der vorzuhaltenden Ortungsinformation offen. Die Bezeichnung als „Streckenfunktion“ wird dem generischen Anspruch nicht gerecht, da Ortsinformationen auch auf dem Zug unabhängig von Streckeneinrichtungen, z.B. mit Satellitenortungssystemen, ermittelt werden können. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*location balise* *(Balisen (Kilometersteine))*		
L	*B*	*D*	*f*	*Provide wayside train protection* *(streckenseitige Zugbeeinflussung)*	Aus betrieblicher Sicht ist der Zweck der Zugbeeinflussung interessant. Dieser ist in dem Begriff „Zugbeeinflussung“ enthalten, aber nicht formuliert worden.	Bv

Ergänzungen zur prEN 15380-4 [BEP08]						Beurteilung der funktionalen Relevanz für Betriebsverfahren (Bv)	
CODE			f	Function (DE)		Erläuterung / Anmerkung	Zuordnung
			e	Example/Explanation (DE)			
			e	*Eurobalise* *(Balisen, Indusi-Magneten, Kabellinienleiter)*		→ funktional dem Bereich der Betriebsverfahren zuzuordnen	
L	*B*	*E*	*f*	*Provide operational telecommunication* *(Betriebsfernmeldeanlagen)*		Telekommunikationseinrichtungen sind technische Hilfsmittel, die bei der Ausführung betrieblicher Funktionen zum Einsatz kommen können. Aus betrieblicher Sicht bleiben in der Formulierung der Zweck und die beabsichtigten Ziele der vorzuhaltenden Einrichtungen offen. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*commercial telecommunication system* *(Beschallungs- und Wechselsprechanlagen, Melde- und Überwachungssysteme, betriebliche Gefahrenmeldeanlagen, Videotechnik, Zugfunk)*			
L	*B*	*F*	*f*	*Control switches* *(Bewegliche Fahrwegelemente sichern)*		Das Stellen von beweglichen Fahrwegelementen ist ein betrieblicher Vorgang, der sich aus der grundlegenden Eigenschaft spurgeführter Verkehrssysteme zur fahrwegseitigen Lenkung von Fahrzeugen ergibt. Dazu werden die beweglichen Fahrwegelemente in die für eine Fahrt benötigte Lage gebracht, die sie für die Dauer der Beanspruchung „sicher“ beibehalten müssen. „Sichern“ ist nur ein Teil der betrieblichen Funktion; der englische Begriff „control“ ist diesbezüglich umfassender und zutreffender. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*switch control, derailer (track locks)* *(Weichen, Gleissperren)*			
L	*B*	*G*	*f*	*Supervise level crossing* *(BÜ sichern)*		Das Sichern von Bahnübergängen ist ebenfalls ein betrieblicher Vorgang. In diesem Fall wird die Funktion mit der deutschen Übersetzung besser getroffen, da er gleichermaßen auf technisch als auch auf nicht technisch gesicherte Bahnübergänge zutrifft. Das englische „supervise“ suggeriert mehr die technischen Realisierungen. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*activation, deactivation, monitoring signal* *(Einschaltung, Ausschaltung, Überwachungssignal)*			

L	*B*	*H*	*f*	*Show correct proceed aspect (Korrektes Fahrsignal anzeigen)*	Das Anzeigen eines Fahrtbegriffs ist eine Realisierungsmöglichkeit für eine betriebliche Funktion im Sinne von „Erteilen der Fahrterlaubnis“. Das Erteilen einer Fahrterlaubnis kann auch mündlich erfolgen. An die Realisierung ist die Anforderung zu stellen, dass der Fahrtbegriff korrekt übertragen wird. → funktional dem Bereich der Betriebsverfahren zuzuordnen	Bv
			e	*signaling systems (Stellbare Signale)*		

Ergebnis: Die L-Funktionen sind sämtlich den Betriebsverfahren zuzuordnen.

Anhang 5: Liste generischer Betriebsverfahrensfunktionen (Auszug FWS)

Bei der folgenden Liste handelt sich um ein Beispiel, wie eine solche Liste aufgebaut sein kann. Die abgestufte Struktur orientiert sich an jener der prEN 15380-4. Je nach Erfordernis des Anwenders kann der Umfang reduziert oder um zusätzlich in der Datenbank abgelegte Informationen, z.B. zu gefährlichen Ergebnissen oder zu Funktionsrealisierungen erweitert werden. Bei umfangreicheren Angaben, die die Möglichkeiten einer tabellarischen Darstellung überschreiten, können „Funktionssteckbriefe“ eine Darstellungsform sein (s.a. Anhang 8).

Nummer und Funktionsname			**Zweck**	**Ergänzende Erläuterung / Klassifizierung**		**Output**		**Benötigter Input**
			Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	Fahrwegsicherung		… einen freien Fahrweg einzustellen und gegenüber anderen Fahrzeugen / Fahrzeugverbänden sowie querenden Dritten zu sichern.	Die zwischen einem Start- und einem Zielpunkt liegenden Fahrwegelemente müssen frei von anderen Beanspruchungen sein, d.h. andere Beanspruchungen ausgeschlossen sein (FWS-1). Die beweglichen Fahrwegelemente müssen sich in der erforderlichen Lage befinden (FWS-2) und der Fahrweg gegen kreuzende Dritte gesichert sein (FWS-3).	Fgr	Gesicherter Fahrweg	„Fahrweg ist gesichert“	s. zugehörige Funktion
FWS	1	Ausschluss konkurrierender Fahrwegelementbeanspruchung	… untereinander unverträgliche Beanspruchungen von Fahrwegelementen durch Fahrzeuge oder Fahrzeugverbände auszuschließen.	Der Ausschluss konkurrierender Beanspruchungen beruht auf einer Entscheidung über die Zulässigkeit beabsichtigter Beanspruchungen und dem Befolgen der Entscheidung. Ein Fahrwegelement darf nur zur Beanspruchung freigegeben werden, wenn es frei von anderen Beanspruchungen ist. Dazu müssen alle Formen der Fahrwegelementbeanspruchung ermittelt (FWS-1.1) und über die Zulassung einer neuen Beanspruchung entschieden werden (FWS-1.2).	BGrF	Ausschluss konkurrierender Fahrwegelementbeanspruchung	"konkurrierende Beanspruchung ist ausgeschlossen"	Summe des Inputs der zugeordneten Teilfunktionen

[45] AbF = Abfangfunktion, BGrF = Betriebliche Grundfunktion, BTf = Betriebliche Teilfunktion , Fgr = Funktionsgruppe, PrKoF = Prüf- und Kontrollfunktion, SchF = Schadensbegrenzungsfunktion, sonF = sonstige Funktion, SubF = Subsystemfunktion

Nummer und Funktionsname					Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
					Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	1	1	Beanspru-chungsermittlung		… alle Formen der Beanspruchung von Fahrwegelementen durch andere Fahrzeuge / andere Fahrzeugverbände zu erfassen.	Zum Ausschluss konkurrierender Fahrwege müssen alle Formen der Fahrwegbeanspru-chung ermittelt werden. In Abhängigkeit davon, wo sich das nutzende Fahrzeug befindet, ergeben sich unterschiedliche Beanspruchungsformen: Fahrzeug auf dem Fahrwegelement (FWS-1.1.1), Fahrzeug in Annäherung an das Fahrwegelement (FWS-1.1.2), Inanspruchnahme benachbarter lichter Räume (FWS-1.1.3).	BTf	Wert des Beanspruchungs-zustands	"Fahrwegelement nicht beansprucht" "Fahrwegelement beansprucht"	Summe des Inputs der zugeordneten Teilfunktionen
FWS	1	1	1	Besetzungs-ermittlung	… Fahrzeuge / Fahrzeugverbände zu erfassen, die sich physikalisch auf den Fahrwegelementen befinden.	Ein Fahrwegelement ist besetzt, wenn sich ein Fahrzeug / ein Fahrzeugverband unabhängig vom Fahrzustand physikalisch auf ihm befindet.	BTf	Wert des Besetzungszu-stands	"Fahrwegelement nicht (von anderen Fahrzeugen) besetzt" " "Fahrwegelement (von anderen Fahrzeugen) besetzt"	ermittelte Fahrwegelemente physikalische Zustände "Fahrzeug auf Element" oder "kein Fahrzeug auf Element"
FWS	1	1	2	Belegungs-ermittlung	… Fahrwegelementnut-zungen zu erfassen, die sich ergeben, ohne dass sich ein Fahrzeug / Fahrzeugverband physikalisch auf dem Fahrwegelement befindet.	Ein Fahrwegelement ist belegt, wenn ein Fahrzeug / ein Fahrzeugverband für die Fahrt auf ihm zugelassen ist, sich aber noch in der Annäherung befindet. Mit dem physikalischen Erreichen geht die Belegung in die Besetzung über.	BTf	Wert des Belegungszu-stands	"Fahrwegelement nicht (von anderer Fahrt) belegt" "Fahrwegelement (von anderer Fahrt) belegt"	ermittelte Fahrwegelemente logische Belegungsinforma-tion

Nummer und Funktionsname					Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
					Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	1	1	3	Profilkonflikt-ermittlung	… bei benachbarten Gleisen Überschneidungen der jeweils für den Fahrzeugdurchgang benötigten Querschnittsprofile auszuschließen.	Bei Überbreiten von Fahrzeugen oder deren Ladungen können Fahrwegelemente eines benachbarten Gleises beansprucht werden.	BTf	Wert des Profilkonfliktzustands	„kein Profilkonflikt (mit Fahrzeugen im Nachbargleis)" „Profilkonflikt (mit Fahrzeugen im Nachbargleis)"	ermittelte Fahrwegelemente Fahrwegelemente der benachbarten Gleise Gleisabstände Fahrzeugprofile der beteiligten Fahrzeuge
FWS	1	2		Beanspruchungsentscheidung	… die als nicht beansprucht erkannten Fahrwegelemente für die Fahrwegbildung freizugeben.	Hat die Beanspruchungsermittlung ergeben, dass ein Fahrwegelement frei von Beanspruchungen durch andere Fahrzeuge ist, kann es für die Fahrwegbildung freigegeben werden.	BTf	Freigabeentscheidung	„Fahrwegelement (für neue Beanspruchung) freigegeben“ „Fahrwegelement (für neue Beanspruchung) nicht freigegeben"	ermittelte Fahrwegelemente Ergebnis(se) der Beanspruchungsprüfung
FWS	2			Fahrwegeinstellung	… die für die Fahrt eines Fahrzeugs / Fahrzeugverbandes benötigte Lage der beweglichen Fahrwegelemente einzustellen	Um einen die beweglichen Fahrwegelemente eines Fahrwegs einzustellen, muss ein Stellauftrag gegeben (FWS-2.1) und ausgeführt werden (FWS-2.2). Bewegliche Fahrwegelemente brauchen nur dann gestellt zu werden, wenn ihre Ist-Lage nicht bereits der Soll-Lage entspricht. Bewegliche Fahrwegelemente, die die Soll-Lage erreicht haben, dürfen diese bis zum Ende der Beanspruchung nicht mehr verlassen.	BGrF	Eingestellter Fahrweg (Zustand)	Ist-Lagen = Soll-Lagen	Summe des Inputs der zugeordneten Teilfunktionen

Nummer und Funktionsname				Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
				Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	2	1	Stellauftragserteilung	… das Stellen eines beweglichen Fahrwegelements auszulösen.	Ein Stellauftrag darf nur gegeben werden, wenn für das zu stellende Fahrwegelement eine Freimeldung vorliegt.	BTf	Stellauftrag mit Soll-Lage-Wert	Stellauftrag mit Soll-Lage-Wert	Ermitteltes Fahrwegelement Freimeldung für das Fahrwegelement Ermittelte Soll-Lage
FWS	2	2	Soll-Lage herstellen	… die für die Fahrt erforderliche Lage eines beweglichen Fahrwegelements zu erhalten.	Umsetzen des Stellbefehls.	BTf	Lagezustand	Soll-Lage (Zustand)	Stellbefehl mit Soll-Lage
FWS	3		Sicherung von Kreuzungen mit Dritten	… Kreuzungen mit anderen Verkehrswegen zu sichern.	Die Sicherung niveaugleicher Kreuzungen ist i.d.R. eine Gemeinschaftsaufgabe der Eisenbahn und des kreuzenden Verkehrs. Die Teilaufgaben können je nach Einsatzgebiet sehr unterschiedlich gelöst werden. Deshalb wird in der Liste nach vier Einsatzgebieten unterschieden (FWS-3.1), (FWS-3.2), (FWS-3.3), (FWS-3.4); Realisierungen werden dadurch jedoch nicht vorgegeben.	Fgr	Gesicherte Kreuzung mit Dritten	--	--
FWS	3	1	Bahnübergangssicherung	… für die Dauer der Beanspruchung durch die Fahrt einer Bahn die Inanspruchnahme der Kreuzung durch den Straßenverkehr auszuschließen.	Als Bahnübergang wird die Kreuzung einer Eisenbahn mit einem Verkehrsweg verstanden, der dem Straßenverkehr zuzurechnen ist. Dies schließt nichtmotorisierte Verkehre und straßenähnliche Wege ein. Seine Sicherung muss durch eine Anforderung initialisiert (FWS-3.1.1) und ausgeführt (FWS-3.1.2) werden.	BGrF	Gesicherter Bahnübergang (Zustand)	Gesicherter Bahnübergang (Zustand)	Summe des Inputs der zugeordneten Teilfunktionen

Nummer und Funktionsname					Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
					Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	3	1	1	Sicherungs-anforderung	… den Sicherungsvorgang zu initialisieren.	Der Bahnübergang kann nur gesichert werden, wenn die Sicherung vor der Inanspruchnahme durch eine Eisenbahn aus dem Betrieb heraus angefordert wird.	BTf	Sicherungsanfor-derung	Sicherungsanforde-rung	Ermitteltes Fahrwegelement mit BÜ Betriebliche Information zur Fahrt (Ankündi-gung)
FWS	3	1	2	Sicherungs-vorgang	… den gesicherten Zustand herzustellen.	Nach der Anforderung laufen die Sicherungs-vorgänge ab.	BTf	Gesicherter Bahnübergang (Zustand)	Gesicherter Bahnübergang (Zustand)	Sicherungsanfor-derung
FWS	3	2	Kreuzung mit anderen Schienenbahnen sichern		… für die Dauer der Beanspruchung durch die Fahrt einer Eisenbahn die Inanspruchnahme der Kreuzung durch eine andere Schienenbahn auszuschließen.	Als Kreuzung mit einer anderen Schienenbahn wird die Kreuzung einer Eisenbahn mit einem Verkehrsweg verstanden, der einem anderen Bahnsystem zuzurechnen ist. Ihre Sicherung muss durch eine Anforderung initialisiert (FWS-3.2.1) und ausgeführt (FWS-3.2.2) werden.	BGrF	Gesicherte Kreuzung (Zustand)	Gesicherte Kreuzung (Zustand)	s. Teilfunktionen
FWS	3	2	1	Sicherungs-anforderung	…den Sicherungsvorgang zu initialisieren.	Die Kreuzung mit einer anderen Schienenbahn kann nur gesichert werden, wenn die Sicherung vor der Inanspruchnahme durch eine Eisenbahn aus dem Betrieb heraus angefordert wird.	BTf	Sicherungsanfor-derung	Sicherungsanforde-rung	Ermitteltes Fahrwegelement mit Kreuzung mit anderer Schienenbahn Betriebliche Information zur Fahrt (Ankündi-gung)
FWS	3	2	2	Sicherungs-vorgang	… den gesicherten Zustand zu erreichen.	Nach der Anforderung laufen die Sicherungs-vorgänge ab.	BTf	Gesicherte Kreuzung (Zustand)	Gesicherte Kreuzung (Zustand)	Sicherungsanfor-derung

Nummer und Funktionsname					Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
					Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	3	3	Niveaugleichen Bahnsteigzugang sichern		… für die Dauer der Beanspruchung durch die Fahrt einer Eisenbahn die Inanspruchnahme von Bahnsteigzugängen auszuschließen.	Als Bahnsteigzugang werden höhengleiche Querungen, die keine Bahnübergänge sind, verstanden, die von systemfremden Personen genutzt werden dürfen. Seine Sicherung muss durch eine Anforderung initialisiert (FWS-3.3.1) und ausgeführt (FWS-3.3.2) werden.	BGrF	Gesicherter Bahnsteigzugang (Zustand)	Gesicherter Bahnsteigzugang (Zustand)	s. Teilfunktion
FWS	3	3	1	Sicherungs-anforderung	…den Sicherungsvorgang zu initialisieren.	Ein Bahnsteigzugang kann nur gesichert werden, wenn die Sicherung vor der Inanspruchnahme durch eine Eisenbahn aus dem Betrieb heraus angefordert wird.	BTf	Sicherungsanfor-derung	Sicherungsanforde-rung	Ermitteltes Fahrwegelement mit Bahnsteigzu-gang Betriebliche Information zur Fahrt (Ankündi-gung)
FWS	3	3	2	Sicherungs-vorgang	… den gesicherten Zustand zu erreichen.	Nach der Anforderung laufen die Sicherungs-vorgänge ab.	BTf	Gesicherter Bahnsteigzugang (Zustand)	Gesicherter Bahnsteigzugang (Zustand)	Sicherungsanfor-derung
FWS	3	4	Sonstige Querungen mit dem Fahrweg sichern		… für die Dauer der Beanspruchung durch die Fahrt einer Eisenbahn die Inanspruchnahme der Kreuzung durch Personen auszuschließen.	Unter sonstigen Querungen werden über Gleise führende Dienstwege o,ä. verstanden. Sie dürfen nur von Betriebspersonal genutzt werden. Ihre Sicherung muss durch eine Anforderung initialisiert (FWS-3.4.1) und ausgeführt (FWS-3.4.2) werden.	BGrF	Gesicherte sonstige Querung (Zustand)	Gesicherte sonstige Querung (Zustand)	s. Teilfunktionen
FWS	3	4	1	Sicherungs-anforderung	…den Sicherungsvorgang zu initialisieren	Eine sonstige Querung kann nur gesichert werden, wenn die Sicherung vor der Inanspruchnahme durch eine Eisenbahn aus dem Betrieb heraus angefordert wird.	BTf	Sicherungsanfor-derung	Sicherungsanforde-rung	Ermitteltes Fahrwegelement mit sonstiger Querung Betriebliche Information zur Fahrt (Ankündi-gung)

Nummer und Funktionsname					Zweck	Ergänzende Erläuterung / Klassifizierung		Output		Benötigter Input
					Ausführung, um …	Abkürzungen s. Fußnote[45]		Bezw. Ergebnis	Zul. Ergebniswerte	
FWS	3	4	2	Sicherungs-vorgang	… den gesicherten Zustand zu erreichen.	Nach der Anforderung laufen die Sicherungs-vorgänge ab.	BTf	Gesicherte sonstige Querung (Zustand)	Gesicherte sonstige Querung (Zustand)	Sicherungsanfor-derung

Anhang 6: Hinweise zur Funktionsgruppe FWS

Zu FWS-1 „Ausschluss konkurrierender Fahrwege“

Die Konkurrenz von Fahrwegen gilt nicht nur für die Dauer der Fahrten, sondern beginnt mit ihrem Einstellen. Der Ausschluss konkurrierender Fahrwege wird erreicht, indem für eine Fahrt nur dann ein Fahrweg eingestellt und freigegeben werden darf, wenn dessen Elemente nicht von einer anderen Fahrt beansprucht werden. Dazu muss der Beanspruchungszustand der Fahrwegelemente festgestellt (FWS-1.1) und in Abhängigkeit vom Ergebnis über die Freigabe entschieden werden (FWS-1.2). Dieses zweistufige Grundprinzip lässt sich nicht nur in technischen Sicherungssystemen wiederfinden, sondern auch in Verfahren, wie dem Zugmeldeverfahren. Es trifft aber auch auf das nordamerikanische Sicherungsverfahren „Timetable und Train Order“ zu, bei dem die Feststellung der Beanspruchung durch Zeitabstände realisiert wird: Beim Unterschreiten eines bestimmten Zeitabstands wird ein Abschnitt als beansprucht festgestellt und gegen eine Freigabe entschieden; nach Verstreichen des Zeitabstands gilt der Abschnitt als „frei“ und darf befahren werden.

Beim Feststellen der Beanspruchung eines Abschnitts durch andere Fahrzeuge müssen drei unterschiedliche Beanspruchungsformen beachtet werden, die Ausschlüsse nach sich ziehen und deshalb beherrscht werden müssen. Wegen ihrer zentralen Bedeutung für die Sicherheit ist es angebracht, sie als einzelne generische Funktionen aufzuführen, auch wenn ihre Realsierung u.U. in einem Funktionsträger zusammenfallen kann:

- „Direkte Beanspruchung“: Ein Fahrzeug / der Fahrzeugverband befindet sich physikalisch auf dem Gleisabschnitt. Ob es fährt oder steht ist unerheblich. Dieser Zustand kann durch technische Einrichtungen, wie z.B. Gleisstromkreise oder Achszähleinrichtungen oder auch durch Inaugenscheinnahme erfasst werden. → FWS-1.1.1 „Besetzungsprüfung“
- „Logische Beanspruchung“: Ein Fahrzeug / der Fahrzeugverband ist für die Fahrt in diesen Abschnitt zugelassen, befindet sich aber noch in der Annäherung. Im Gegensatz zur physikalischen Beanspruchung kann diese Beanspruchung nicht unmittelbar durch technische Einrichtungen, sondern nur logisch erfasst werden. → FWS-1.1.2 „Belegungsprüfung“
- „Indirekte Beanspruchung“: Ein Fahrzeug / ein Fahrzeugverband beansprucht z.B. seiner eigenen oder der Breite seiner Ladung wegen den von einem anderen Fahrzeug benötigten lichten Raum eines Nachbargleises. Dann steht das Nachbargleis der anderen Fahrt nicht zur Verfügung. → FWS-1.1.3 „Profilkonfliktprüfung“

Anhang 7: Beispiele für die Analyse definierter Funktionen

Weitere Beispiele zu Abschnitt 5.2

Beispiel „LBE Provide operational telecommunication“

Die Funktion “Provide operational telecommunication” dient grundsätzlich der Übertragung von Informationen von einer Quelle zu einer Senke. Da zwischen den Funktionen eines Systems stets Informationen ausgetauscht werden müssen, ist das Übertragen von Informationen als generisch anzusehen. Es wird davon ausgegangen, dass derartige Übertragungsfunktionen, abgesehen von einer eventuellen Ausgabe der Informationen in einem anderen Medium, keine eigenständigen inhaltlichen Ergebnisse erzeugen und dass somit der an der Quelle in die Übertragungsfunktion eingehende mit den an der Senke aus ihr ausgehenden Inhalt identisch ist. Eine Übertragungsfunktion wird deshalb nicht als betriebliche Grundfunktion angesehen, sondern wird als ein Teil von ihr eingestuft.

→ Zweck: Ausführung, um betriebliche Informationen von einer Quelle zu einer Senke zu übertragen

→ Klassifizierung: Betriebliche Teilfunktion (BTf)

→ Abgleich mit Funktionen gemäß 5.1: Teil jeder Funktion, deren Output an einer Schnittestelle zu übertragen ist

Beispiel „LBF Control switches“

In [BEP08, S.205] wird als deutsche Übersetzung „Bewegliche Fahrwegelemente sichern“ angegeben. Es wird davon ausgegangen, dass mit dieser Funktion nicht nur das Sichern der Lage eines beweglichen Fahrwegelements, sondern dem englischen Verb „to control“ entsprechend umfassender das Ansteuern, Regeln und Prüfen der Lagen beweglicher Fahrwegelemente verstanden werden soll. Dies entspräche der im Abschnitt 5.1.3, Bild 40 aufgeführten Funktion FWS-2 „Fahrwegeinstellung“, die ausgeführt wird, um die für die Fahrt eines Fahrzeugs / Fahrzeugverbandes benötigte Lage der beweglichen Fahrwegelemente einzustellen (vgl. Anhang 5). Diese wird als betriebliche Grundfunktion betrachtet, die nach der Zuteilung der beweglichen Fahrwegelemente durch die den Ausschluss konkurrierender Fahrwegelementbeanspruchungen gewährleistende Funktion FWS-1 ablaufen kann.

→ Zweck: Ausführung, um die für die Fahrt eines Fahrzeugs / Fahrzeugverbandes benötigte Lage der beweglichen Fahrwegelemente einzustellen.

→ Klassifizierung: Betriebliche Grundfunktion (BGrF)

→ Abgleich mit Funktionen gemäß 5.1: entspricht FWS-2 „Fahrwegeinstellung“

Beispiel „LBG Supervise level crossing“

Diese Funktion wird mit den Begriffen activation, deactivation und monitoring signal ergänzend beschrieben. Sie soll folglich den gesamten Prozess von der Aktivierung bis zur Beendigung umfassen. Sie entspricht damit im Prinzip der Funktion FWS-3.2, die ausgeführt

werden soll, um für die Dauer der Beanspruchung durch die Fahrt einer Bahn die Inanspruchnahme der Kreuzung durch den Straßenverkehr auszuschließen. Diese Definition enthält keinen Hinweise auf ein Überwachungssignal, da die Verwendung eines solchen eine Frage der Realisierung ist. Es hätte innerhalb einer entsprechenden Systemlösung für FWS-3.2 die Bedeutung einer Prüf- und Kontrollfunktion.

→ Zweck: Ausführung, um für die Dauer der Beanspruchung durch die Fahrt einer Bahn die Inanspruchnahme der Kreuzung durch den Straßenverkehr auszuschließen.

→ Klassifizierung als betriebliche Grundfunktion (BGrF)

→ Abgleich mit Funktionen gemäß 5.1: entspricht FWS-3.2

Beispiel „LBH Show correct proceed aspect"

Das Verb „to show" unterstreicht den Aspekt des Anzeigens, des Ausgebens. Die Funktion soll folglich ausgeführt werden, um Fahrtbegriffe von einer fahrtzulassenden an eine fahrtsteuernde Instanz zu übertragen. Dass dieses korrekt, d.h. fehlerfrei geschehen muss, ist für zugelassene Systeme eine elementare Anforderung, die keines ergänzenden Hinweises bedarf. Der zur Fahrtzulassung führende Prozess wird nicht als Bestandteil der hier definierten Funktion aufgefasst. Da „to show" und auch das deutsche „anzeigen" auf visuell geprägte Systemlösungen abzielen, sollte im Hinblick auf andere Lösungsmöglichkeiten das Verb „to transmit" verwendet werden.

→ Zweck: Ausführung, um Fahrtbegriffe von einer fahrtzulassenden Instanz an eine fahrtsteuernde Instanz zu übertragen.

→ Klassifizierung im Sinne einer Übertragungsfunktion als betriebliche Teilfunktion (BTf), vgl. auch Funktion LBE

→ Abgleich mit Funktionen gemäß 5.1: Teil der Funktionsgruppe ERL „Fahrterlaubnis und Restriktionen erteilen"

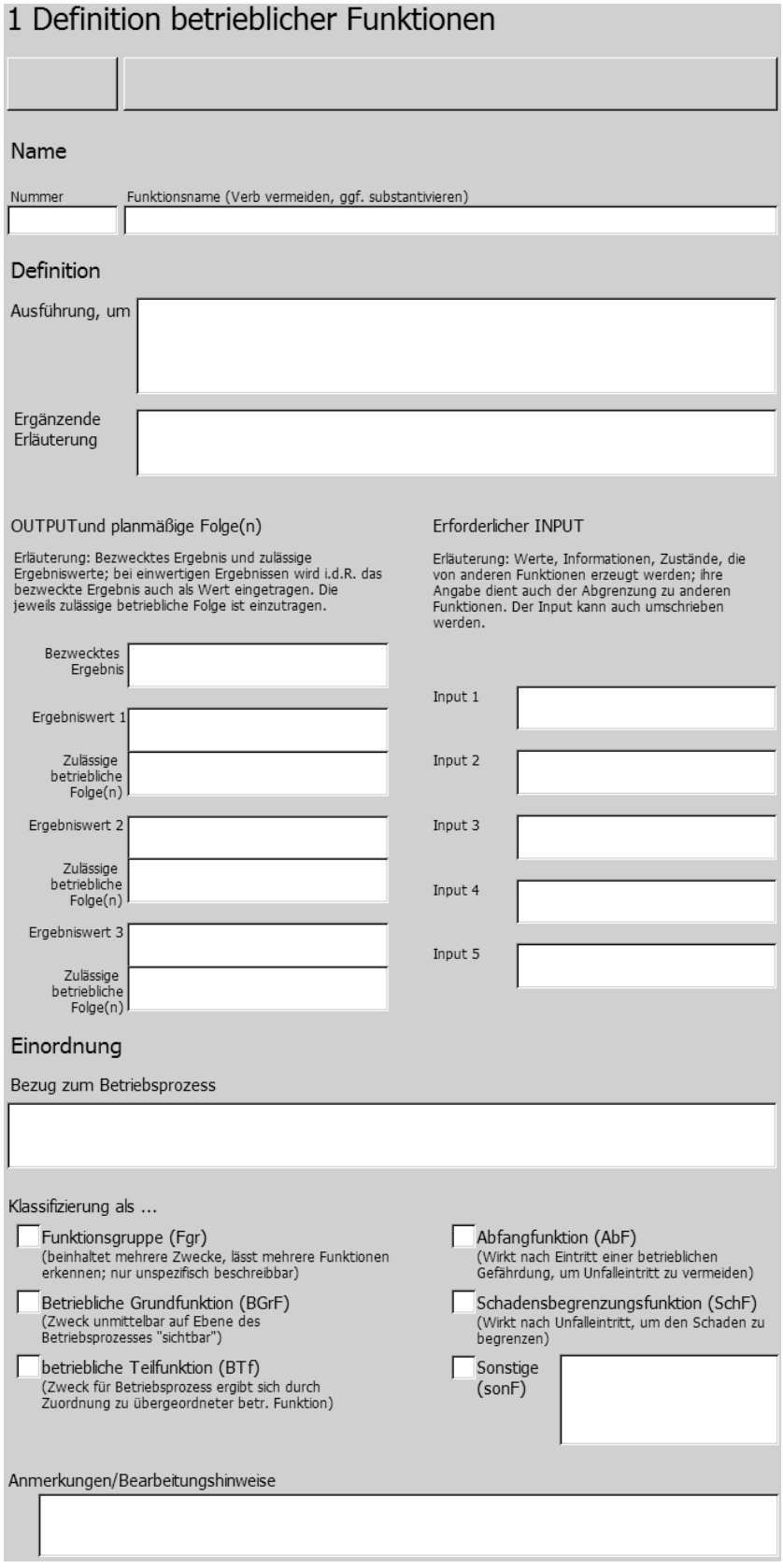
Anhang 8: Funktionssteckbrief (Beispiel)

In dieser Anlage wird dargestellt, wie ein Funktionssteckbrief aufgebaut und welchen Inhalts er sein könnte.

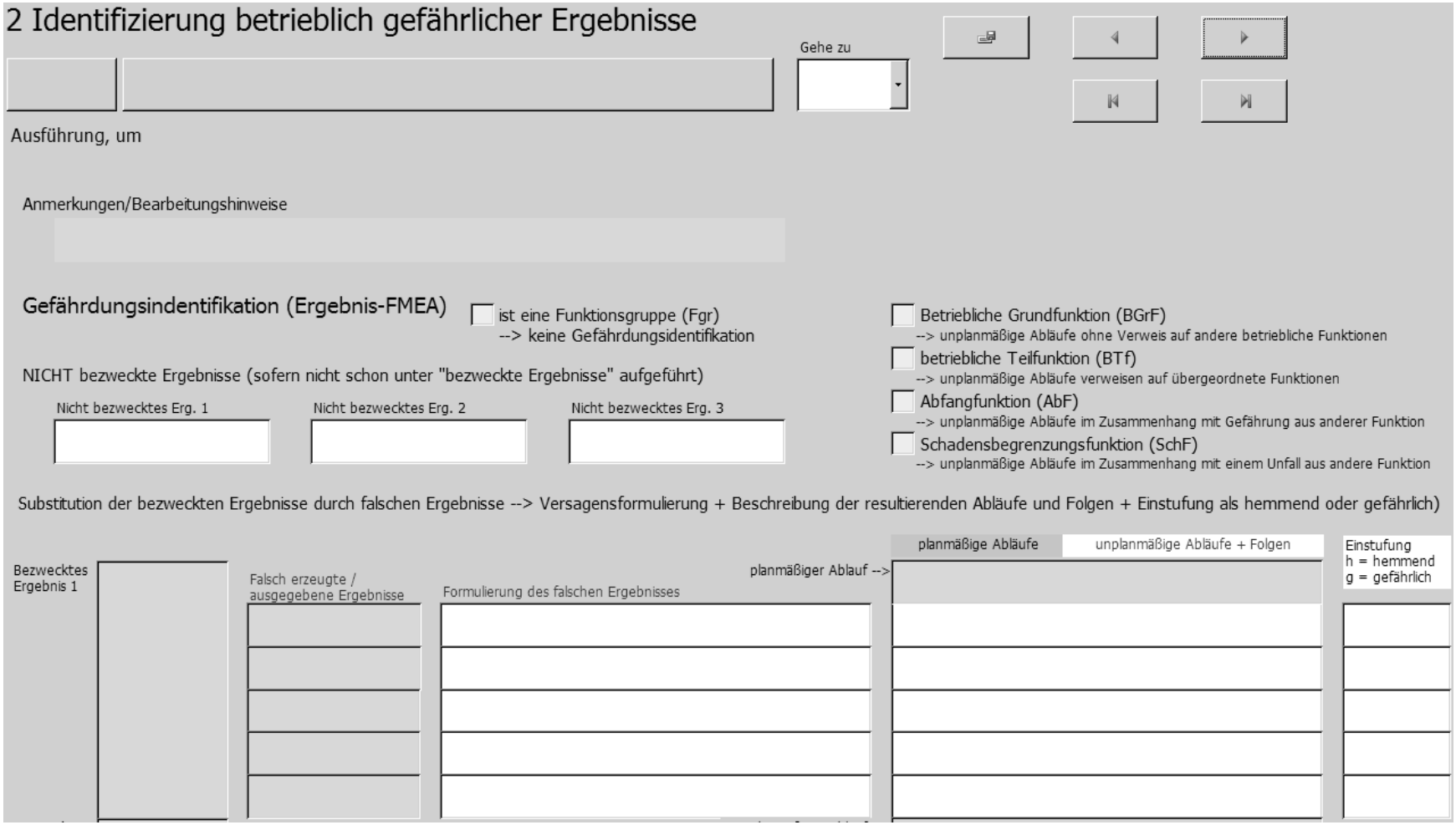
<table>
<tr><td colspan="4">Definition, Beschreibung, Input</td><td colspan="2">Einordnung als</td><td>Betriebliche Teilfunktion (BTf) der Grundfunktion FWS-1</td></tr>
<tr><td>Funktion</td><td colspan="3">FWS 1.1 Beanspruchungsermittlung</td><td rowspan="2">Über-geordnet</td><td>Funktions-gruppe</td><td>FWS Fahrwegsicherung
Ausführung, um einen freien Fahrweg einzustellen und gegenüber anderen Fahrzeugen / Fahrzeugverbänden sowie querenden Dritten zu sichern.</td></tr>
<tr><td>Ausführung, um …</td><td colspan="3">… alle Formen der Beanspruchung von Fahrwegelementen durch andere Fahrzeuge / andere Fahrzeugverbände zu erfassen.</td><td>Grund-funktion</td><td>FWS-1 Ausschluss konkurrierender Fahrwegelementbeanspruchung
Ausführung, um untereinander unverträgliche Beanspruchungen von Fahrwegelementen durch Fahrzeuge oder Fahrzeugverbände auszuschließen.</td></tr>
<tr><td>Ergebnis</td><td colspan="3">Wert des Beanspruchungszustands</td><td rowspan="5">Unter-geordnet</td><td rowspan="5">Teil-funktionen</td><td>FWS-1.1.1 Besetzungsermittlung
Ausführung, um Fahrzeuge / Fahrzeugverbände zu erfassen, die sich physikalisch auf den Fahrwegelementen befinden.</td></tr>
<tr><td>Zul. Ergebniswerte</td><td>"Fahrwegelement nicht beansprucht"</td><td colspan="2">"Fahrwegelement beansprucht"</td><td rowspan="2">FWS-1.1.2 Belegungsermittlung
Ausführung, um Fahrwegelementnutzungen zu erfassen, die sich ergeben, ohne dass sich ein Fahrzeug / Fahrzeugverband physikalisch auf dem Fahrwegelement befindet.</td></tr>
<tr><td>Zul. betriebl. Folgen</td><td>Fahrt</td><td colspan="2">Abweisung einer beabsichtigten Beanspruchung</td></tr>
<tr><td>Ergänzende Erläuterung</td><td colspan="3" rowspan="2">Zum Ausschluss konkurrierender Fahrwege müssen alle Formen der Fahrwegbeanspruchung ermittelt werden. In Abhängigkeit davon, wo sich das nutzende Fahrzeug befindet, ergeben sich unterschiedliche Beanspruchungsformen: Fahrzeug auf dem Fahrwegelement (FWS-1.1.1), Fahrzeug in Annäherung an das Fahrwegelement (FWS-1.1.2), Inanspruchnahme benachbarter lichter Räume (FWS-1.1.3).</td><td>FWS-1.1.3 Profilkonfliktermittlung
Ausführung, um bei benachbarten Gleisen Überschneidungen der jeweils für den Fahrzeugdurchgang benötigten Querschnittsprofile auszuschließen.</td></tr>
<tr><td rowspan="5">Benötigter Input; Ursprung der Inputs</td><td colspan="2">ermittelte Fahrwegelemente</td><td>von EF-1</td><td rowspan="2">Hinweise zur Einordnung</td><td rowspan="2">Der Bezug zum Betriebsprozess ergibt sich mittelbar über die übergeordnete Funktion, die dem Ausschluss konkurrierender Beanspruchungen dient. FWS-1.1 wird deshalb als Betriebliche Teilfunktion eingestuft.</td></tr>
<tr><td colspan="2">Wert des Besetzungszustands</td><td>von FWS-1.1.1</td></tr>
<tr><td colspan="2">Wert des Belegungszustands</td><td>von FWS-1.1.2</td><td rowspan="3">Beispiel</td><td rowspan="3">Zusammenwirken der Ergebnisse einer Gleisfreimeldeanlage, der Festlegung der Fahrstraße in einem Stellwerk und den Ergebnissen der Behandlung von Lademaßüberschreitungen durch einen Fahrdienstleiter.</td></tr>
<tr><td colspan="2">Wert des Profilkonfliktzustands</td><td>von FWS-1.1.3</td></tr>
<tr><td colspan="2">--</td><td>von --</td></tr>
<tr><td colspan="4">Falsche Ergebnisse und Folgen</td><td colspan="2"></td></tr>
<tr><td>Gefährlich</td><td colspan="2">Für ein Fahrwegelement wird keine Beanspruchung ausgegeben, obwohl es beansprucht ist.</td><td colspan="3">Mehrere Unfallarten möglich: z.B. Entgleisungen wg. Umstellen von Fahrwegelementen vor/unter einem anderen Zug; Kollisionen mit Fahrzeugen im eigenen Gleis oder bei Fahrten in das Nachbargleis</td></tr>
<tr><td>Hemmend</td><td colspan="2">Für ein Fahrwegelement wird eine Beanspruchung ausgegeben, obwohl es nicht beansprucht ist.</td><td colspan="3">Eine zulässige Fahrt findet nicht statt.</td></tr>
</table>

Anhang 9: Eingabemasken

Beispiel für eine Eingabemaske zur Definition betrieblicher Funktionen (Screenshot)



Beispiel für eine Substitutionstabelle (Sreenshot, Auszug)



Abkürzungsverzeichnis

AbF	Abfangfunktion
A.d.V.	Anmerkung des Verfassers
ATO	Automatic Train Operation
ATP	Automatic Train Protection
BAM	Betriebliches Anforderungsmanagement (Projektname)
BGrF	Betriebliche Grundfunktion
BP	Best Practice
BQM	Barrier Quantification Model
BS	Basic System
Bsp.	Beispiel
BTf	Betriebliche Teilfunktion
BÜ	Bahnübergang
Bv	Betriebsverfahren
BvF	Betriebsverfahrensfunktion
bzgl.	bezüglich
CSM	Common Safety Methods
DB AG	Deutsche Bahn Aktiengesellschaft
DEUFRAKO	Deutsch-Französische Kooperation in der Verkehrsforschung
DIN	Deutsches Institut für Normung e.V.
DS	Druckschrift
DV	Dienstvorschrift
CENELEC	Comité Européen de Normalisation Electrotechnique
d.h.	das heißt
e	Example/explanation (engl. Beispiel/Erläuterung)
EBA	Eisenbahn-Bundesamt
EDV	Elektronische Datenverarbeitung
EF	„Ermittlung von Fahrwegelementen“ (Funktionsgruppe)
e.g.	“exempli gratia” (lateinisch); for example
EIU	Eisenbahninfrastrukturunternehmen
EN	Europäische Norm
ERA	European Railway Agency
ERL	„Fahrterlaubnis und Restriktionen erteilen“ (Funktionsgruppe)
ERTMS	European Rail Traffic Management System
ESTW	Elektronisches Stellwerk
ETCS	European Train Control System
EVU	Eisenbahnverkehrsunternehmen
f	function
Fdl	Fahrdienstleiter

FFB	FunkFahrBetrieb
Fgr	Funktionsgruppe
FMEA	Failure Mode and Effects Analysis (Fehler-Möglichkeits- und –Einfluss-Analyse)
FNS	Funktionales Nachbarsystem
FWE	„Fahrwegeignungsprüfung“ (Funktionsgruppe)
FWS	„Fahrwegsicherung“ (Funktionsgruppe)
Fz	Fahrzeug
FzF	Fahrzeugfunktion
ggf.	gegebenenfalls
H	Hazard
ICE	InterCityExpress
i.d.R.	in der Regel
IEC	International Electrotechnical Commission
IfEV	Institut für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig
KF	Kommando-Freigabe
km	Kilometer
LC	Level crossing
LST	Leit- und Sicherungstechnik
LÜ	Lademaßüberschreitung
LZB	Linienförmige Zugbeeinflussung
MS	Microsoft
NF	Neutralising Factors
OW	Ortsgestellte Weiche
prEN	Europäische Vornorm
PZB	Punktförmige Zugbeeinflussung
PrKoF	Prüf- und Kontrollfunktion
RA	Risikoanalyse
Rb	Rangierbegleiter
RBC	Radio Block Center
RCM	Risk Control Model
ROSA	Rail Optimisation Safety Analysis (Projektname)
s.	siehe
SchF	Schadenbegrenzungsfunktion
SIL	Safety Integrity Level
sonF	sonstige Funktion
SPH	Starting Point Hazard (Ausgangsgefährdung)
SPO	Subjekt, Objekt, Prädikat
SP	„Sicherung von Personen“ (Funktionsgruppe)
SubF	Subsystemfunktion

SW	Schrankenwärter
Tf	Triebfahrzeugführer
THR	Tolerable Hazard Rate
TVE	Transrapid Versuchsanlage Emsland
u.a.	unter anderem
UIC	UNION INTERNATIONALE DES CHEMINS DE FER (Internationaler Eisenbahnverband)
UNIFE	Union des Industries Ferroviaires Européennes (Europäischer Verband der Bahnindustrie)
u.U.	unter Umständen
V	Geschwindigkeit
VDV	Verband Deutscher Verkehrsunternehmen
vgl.	vergleiche
vgl. a.	vergleiche auch
wg.	wegen
WP	Wartungspersonal
z.B.	zum Beispiel
z.T.	zum Teil
zul V	Zulässige Geschwindigkeit